NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RISK UNBOUND: THREAT, CATASTROPHE, AND THE END OF HOMELAND SECURITY

by

Jacob S. Anderson

September 2015

Thesis Advisor:	Chris Bellavita
Second Reader:	Lee Clarke

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE RISK UNBOUND: THREAT, CATASTROPHE, AND THE END OF HOMELAND SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Anderson, Jacob S.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Threat and catastrophe highlight the impossibility of providing perfect security, and demonstrate the limitations of risk-based security practices. This thesis presents an argument in three parts. First, the dangers homeland security agencies confront are increasingly beyond the reach of measures for control. The character of security risks is complex and volatile, while worst-case possibilities—not merely probable accidents and disasters—are particularly relevant to domestic security agencies and organizations. Second, the security response to such unbounded risks has been the creation of unconscionable maps—tools and concepts that presume a greater degree of knowledge, uniformity, and control than is available. Finally, there is a body of knowledge and capability better suited to security uncertainties, and homeland security agencies must find ways to cultivate these capacities. Contrary to current security practices, national adaptability is more desirable than perfect knowledge, control of crisis, or national uniformity.

14. SUBJECT TERMS catastrophe, command and control, complexity, crisis, disaster, doctrine, normal accident, risk, risk-based security, risk management, risk society, threat, uncertainty, volatility, worst-cases	**15. NUMBER OF PAGES** 195
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

RISK UNBOUND: THREAT, CATASTROPHE, AND THE END OF HOMELAND SECURITY

Jacob S. Anderson
Senior Policy Analyst, Department of Homeland Security,
National Protection & Programs Directorate, Office of Infrastructure Protection
B.A., Grove City College, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2015**

Author:	Jacob S. Anderson
Approved by:	Chris Bellavita Thesis Advisor
	Lee Clarke Second Reader
	Mohammed Hafez Chair, Department of National Security

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Threat and catastrophe highlight the impossibility of providing perfect security, and demonstrate the limitations of risk-based security practices. This thesis presents an argument in three parts. First, the dangers homeland security agencies confront are increasingly beyond the reach of measures for control. The character of security risks is complex and volatile, while worst-case possibilities—not merely probable accidents and disasters—are particularly relevant to domestic security agencies and organizations. Second, the security response to such unbounded risks has been the creation of unconscionable maps—tools and concepts that presume a greater degree of knowledge, uniformity, and control than is available. Finally, there is a body of knowledge and capability better suited to security uncertainties, and homeland security agencies must find ways to cultivate these capacities. Contrary to current security practices, national adaptability is more desirable than perfect knowledge, control of crisis, or national uniformity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	The Attacks of September 11, 2001
CBP	Customs and Border Protection
CIPA	Critical Infrastructure Protection Act
CMI	Consequence Measurement Index
DHS	Department of Homeland Security
DOT	Department of Transportation
EMP	Electromagnetic Pulse
FEMA	Federal Emergency Management Agency
FIRESCOPE	Firefighting Resources of California Organized for Potential Emergencies
HSPD-5	Homeland Security Presidential Directive 5
HSPD-8	Homeland Security Presidential Directive 8
ICE	Immigration and Customs Enforcement
ICS	Incident Command System
IMAT	Incident Management Assistance Team
IRA	Irish Republican Army
ISC	Interagency Security Committee
NFIP	National Flood Insurance Program
NIMS	National Incident Management System
PMI	Protective Measures Index
PPD-8	Presidential Policy Directive 8
RHIC	Relativistic Heavy Ion Collider
RMI	Resilience Measurement Index
RRF	Rapid Reflection Force
SNRA	Strategic National Risk Assessment
TCE	Threat Credibility Evaluation
TRIA	Terrorism Risk Insurance Act of 2002
TSA	Transportation Security Administration
UK	United Kingdom

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

> *Each of us is all the sums he has not counted...the seed of our destruction will blossom in the desert, the alexin of our cure grows by a mountain rock*
>
> —Thomas Wolfe[1]

The staircases in medieval castles often spiraled upward clockwise around a central newel. The reasoning for this design tendency, so the theory goes, was to give the advantage to the (right-handed) defender, who had more room to swing his sword from above.[2] There is elegance to this idea. Fortifications may be complicated, but the principle of fortification is simple. Thinking about castles this way conjures up images of attackers and defenders, the forces of good arrayed against the forces of evil, civilization versus barbarism and the outer dark. It is a simplicity that homeland security agencies might envy.

The crash of Germanwings 9525 in March of 2015 illustrates a more uneasy insecurity. When the captain left the cockpit during that flight, the co-pilot locked the cabin door and intentionally crashed the aircraft into a mountainside in the French Alps, killing the 144 passengers and 6 crewmembers.[3] The subsequent review of safety protocols in hindsight belies a darker concern: procedures must consider more fully how to protect *against* the pilot. The professional most directly responsible for the safety of the plane must be thought of as a liability. "The irony of risk here," says Ulrich Beck, "is that rationality, that is, the experience of the past, encourages anticipation of the wrong

[1] Thomas Wolfe, *Look Homeward, Angel* (New York, NY: Charles Scribner's Sons, 1929; New York, NY: Simon and Schuster, 2006), 5. Citations refer to the Simon and Schuster edition.

[2] Eugène-Emmanuel Viollet-le-Duc, *Dictionnaire raisonné de l'architecture française du XI au XVI siècle* [dictionary of French architecture from the 11th–16th century] (Paris, FR: A. Morel, 1869), 296.

[3] Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile (BEA), *Rapport préliminaire Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l'Airbus A320-211 immatriculé D-AIPX exploité par Germanwings* [Preliminary Report on the Germanwings Flight 9525 Crash] (Paris, FR: BEA, May, 2015), 11.

kind of risk, the one we believe we can calculate and control, whereas the disaster arises from what we do not know and cannot calculate."[4] This is what it means for risk to be unbound. In the concentrated, unaccountable example of Germanwings, the pilot was able to create astonishing tragedy, not despite complicated fortification, but because of it.

In order to understand the probability and consequence of a risk, the analysis of that risk must establish an area of study and an area of impact. Catastrophe, like the Germanwings crash, has a knack for acquainting security organizations with previously unforeseen dimensions. As Beck points out, what we do not know becomes the central figure in risk decision-making, not what we know. In 2013, through a series of startling and unseen connections, crude oil from the Bakken oil fields in North Dakota exploded during a train derailment, resulting in 47 fatalities in the town of Lac-Mégantic, Quebec. The Lac-Mégantic accident demonstrates the way that complex risks can span political boundaries and professional disciplines, challenging the available tools of risk calculation.[5]

Homeland security risk, it seems, is often not fully risk at all. It remains as uncertainty and danger. And this is at the heart of a modern challenge to risk-based security practices. If homeland security is predominantly in the business of the unlikely, then it is problematic to think of ordering its capabilities against likely outcomes—even a suite of likely outcomes. So, homeland security professionals must consider and decide whether their work is fundamentally about the management of outliers, and what corresponding shifts this recognition requires in doctrine, theory, and practice.

Politics is well said to be the art of the possible.[6] Increasingly, homeland security may be the art of the impossible. Unable to be selective about the risks they are asked to

[4] Beck, Ulrich, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

[5] Transportation Safety Board of Canada, *Railways Investigation Report R13D0054 Runaway and Main-Track Derailment of Montreal, Maine, & Atlantic Railways Freight Train MMA-002 MILE 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013* (Gatineau, QC: August, 2014), 1.

[6] Otto Von Bismarck, *Fürst Bismarck: Neue Tischgespräche und Interviews* [prince Bismarck: new table discussions and interviews] (Stuttgart and Leipzig, DE: Deutsche Verlags-Anstalt, 1895), 248.

manage, homeland security agencies must organize against threats and catastrophes that progressively outstrip efforts at control. The predominant security response has been to either meet the uncertainties of threat and catastrophe with tools designed and better suited for certainty, or address unbounded risks with unbounded precaution. Such arrangements promise a greater degree of security than is possible. Thus, far this has meant that the purpose of homeland security is progressively redefined by perceived failures—as security organizations fail to deliver the promised level of security. However, the wilderness of catastrophic possibility suggests an alternate answer to the question of what the purpose of homeland security could be.

In the insurance industry "adverse selection" occurs when the only purchasers of an insurance product are at an elevated risk of needing it. That is, they are particularly exposed to the threat or hazard being insured against. Adverse selection concentrates risk, and makes it extremely difficult to spread risks or distribute losses, illustrating the plight of homeland security agencies. The only individuals under the protection of the United States Secret Service, for instance, are at an elevated risk of needing such protection. Nor can the Secret Service absorb potential losses. It is difficult to apply traditional risk management concepts to such risks.

Largely, the security response to unbounded risk has been the creation of "unconscionable maps"—tools and concepts that presume a greater degree of knowledge, uniformity, and control than is available. Such maps display two problematic tendencies: the pretense of applying risk management when the information necessary to support such calculation is not available, and boundless precaution. In the first case homeland security lives with a false assumption that it has exerted control over a risk, in the second, homeland security has little assurance or measure of success and surrenders decisions to threat politics.

Unconscionable maps have a tendency to pave over uncertainty—to render organizations insensitive to it. Much of homeland security theory and practice is organized around presumed control, rather than presumed surprise. However, the research of this thesis supports the notion that homeland security theory must develop better tools for living with enduring uncertainty, danger, and possibility.

The operating environment for domestic security is the complex of authorities and jurisdictions inherent to American federalism. Security agencies have tended to treat this networked landscape as a security liability, exploring means to create uniformity in security practices, and even alignment of command and control structures in the wake of disasters. The network of federalism may be a security asset, not a liability. American government functions to decentralize strengths and distribute vulnerabilities, and, while it often stymies attempts at national security architectures, is uniquely positioned to develop adaptive systems for managing uncertain security risks. Federalism provides the architecture for decentralized preparedness, and yet homeland security agencies are pursuing an end state of centralization and uniformity in practice, in the process stifling adaptability and innovation. Centralization—even the centralization of strengths—creates certain vulnerabilities.

As security agencies inherit complex and uncertain risks, they require a corresponding change in approach. Such a shift will require incremental adjustments to unbounded risks, increasing the capacity of security organizations to explore uncertainties and work with uncommon partners. It will also require more dramatic shifts away from heavily scripted plans and the pursuit of the National Incident Management System (NIMS). In place of unilateral security doctrines, homeland security requires a multivalent security doctrine that stresses adaptability over control and uniformity.

The word "end," says Neil Postman, has at least two important meanings: "purpose" and "finish."[7] If the purpose of homeland security is to manage the unmanageable, abandoning a grand design for homeland security may improve our ability to live with danger, and achieve greater security.

[7] Neil Postman, *The End of Education: Redefining the Value of School* (New York, NY: Vintage, Knopf Doubleday Publishing Group, 1996), x.

List of References

Beck, Ulrich. “Living in the World Risk Society.” *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

Bismarck, Otto Von. *Fürst Bismarck: Neue Tischgespräche und Interviews*. Stuttgart and Leipzig, DE: Deutsche Verlags-Anstalt, 1895.

Bureau d’Enquêtes et d’Analyses pour la Sécurité de l’Aviation Civile (BEA). *Rapport préliminaire Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l’Airbus A320-211 immatriculé D-AIPX exploité par Germanwings.* Paris, FR: BEA, May 2015.

Postman, Neil. *The End of Education: Redefining the Value of School*. New York, NY: Vintage, Knopf Doubleday Publishing Group, 1996.

Transportation Safety Board of Canada. *Railways Investigation Report R13D0054: Runaway and Main-Track Derailment of Montreal, Maine, & Atlantic Railways Freight Train MMA-002 MILE 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013*. Gatineau, QC: August 2014.

Viollet-le-Duc, Eugène-Emmanuel. *Dictionnaire raisonné de l’architecture française du XI. au XVI. siècle*. Paris, FR: A. Morel, 1869.

Wolfe, Thomas. *Look Homeward, Angel*. New York, NY: Simon and Schuster, 2006. First published in 1929 by Charles Scribner’s Sons.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

For over a decade now, Rebecca Coffin Anderson has been my wife, best friend, first editor, and most honest critic. She created the time and space necessary to research and write this thesis, and maintained for almost a year the illusion that I wasn't repeating myself or going slightly mad. I love her deeply, and am impossibly grateful for her as well as my three precocious and unusual children for their patience, support, and probing questions.

Chris Bellavita was instrumental in turning this research from a mad idea to a workable thesis. Along the way, his questions were better than answers, and I'm particularly indebted to his unaffected genius, unsettling wisdom, and quiet encouragement.

I admire Lee Clarke's writing and thought so much; I'm not sure what possessed me to ask him to read my own meager work. Lee's insight and clarity are only matched by his generosity, and I'm grateful for the time and thought he has provided to improve and guide my thinking and writing.

The Center for Homeland Defense and Security consists of two classrooms—the faculty and staff who run the program, and the uncommon collection of minds that make up each cohort. This thesis is very much the product of both classrooms.

I owe a great deal to my dad, a fighter pilot whose deceptive calm in the face of uncertainty permeates my thinking in more ways than I can pinpoint, and my mom, who invented the culture of my youth, and forced my siblings and me to read.

The idea for this thesis came about while working disasters with tirelessly adaptive emergency managers like Greg Coulson and Tom Breslin at FEMA. Greg taught me to circumvent the special brand of thick-headedness that can creep into command and control systems. Tom intentionally taught me to write doctrine, and unwittingly taught me that crisis management is art not science, and improvisation not procedure. I am more grateful than he knows for his unconventional leadership.

I must also thank Dr. Eric Potter, professor of English at Grove City College, for gravely taking in the news and then calmly finishing his lecture on American literature that terrible morning in September of 2001. It is an example I still admire.

Ulrich Beck and Raphael Sagarin both died while I was working on this thesis. I have met neither of them, but it would be dishonest not to particularly acknowledge the impact of their writing here as well as in the body of my argument. The world of security is larger for their writing, and smaller with their passing.

While I owe a great debt to the thoughts of many others whose work is referenced in this thesis, the shortcomings in my research and representations of the views of others are, of course, entirely my own.

I. INTRODUCTION

This thesis is critical of established methods and dominant security practices. Done poorly, criticism is an easy task. Done properly, polemic places a special burden of rigor and humility on the writer, both to fairly consider and state the principle and practice he is criticizing, and to acknowledge that even the most flawed practices usually come about from good faith efforts. This thesis is written from a deep well of respect for the responders and operational innovators who have designed and built existing national preparedness systems—as well as those who have worked around them, hacked them, and reformed them. I have labored to faithfully represent the intent and purpose of existing doctrine and theory, and to propose reforms that this research suggests are needful. While I owe an impossible debt to the thoughts of many others whose work is referenced in this thesis, any shortcomings in my research and writing are, of course, entirely my own.

A. RESEARCH QUESTION

Faced with risks that increasingly defy temporal, spatial, social, and rational boundaries, what could be the purpose of homeland security?

Much of the effort of homeland security is a struggle for knowledge and control. But how should homeland security manage what it cannot control? Despite more than a decade of applied expertise under the banner of homeland security, bad things—from tornadoes to terrorism—continue to impact America. Security, we know, will never be absolute, but exists alongside enduring insecurity. Here homeland security professionals must confront basic assumptions about the purpose and final state of domestic security. And in response, should our theory, doctrine and practice refocus away from controlling uncertainty—and toward disciplined irregularity, exploration, and improvisation? Are we to be precautionists or pioneers? Faced with the enduring character of insecurity, catastrophe and uncertainty, how has homeland security responded, and what tools are available to manage the edges of knowledge and control?

I will consider whether the dominant mode of managing these borderlands of capacity has been to presume control over things beyond control, and whether the emphasis on imagination in the wake of the 9/11 Commission report only generated fantasies of control.[8] Pervasive uncertainty and insecurity may require something different of homeland security professionals.

B. PROBLEM STATEMENT

Three dominant pillars of homeland security theory and practice—knowledge of threat and danger, control of crisis, and national uniformity in security practices—have not overcome intractable risks in over a decade of aspiration, suggesting that contemporary security problems are not responsive to these measures.[9]

Analysts are equally unable to predict terrorist attacks, fathom the impact of nuclear or environmental catastrophe, or manage the blossoming complexity of pandemics. This in turn suggests that the homeland security enterprise must earnestly begin to shift its attention, its theory and practice, toward the problem of uncertainty. Uncertainty, then, is not a problem to be eradicated, but is an enduring feature to be lived with.

In this thesis, I will consider how the homeland security enterprise has conceptualized and managed unmapped security situations at the edge of its understanding. I will propose some refinements that move security theory away from aspirations of unattainable degrees of knowledge or total control and toward a view of uncertainty that relies on organizational self-knowledge, improvisation, and exploration in a security wilderness.

[8] Lee Clarke, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago, IL: University of Chicago Press, 1999), 99.

[9] I have in mind here the way security organizations pursue knowledge of threats through crisis situational awareness and risk calculation as well as intelligence collection and analysis. In conditions of high uncertainty, the pursuit of such information is insatiable and organizations often presume to attain greater degrees of knowledge than are available to them. In doing so, they lack a limiting principle to the pursuit of information. Precaution, and boundless pursuit of threat knowledge becomes the dominant mode of security.

In some vital ways, homeland security organizations are not built for such wilderness. They are not structured for it—organizing around presumed control rather than presumed surprise. They are not ready for it—planning and exercising against controlled scenarios. The tools of national preparedness have a utopian character to them, expressing a promise of perfect, real-time awareness of threats, vulnerabilities, and system performances. Conversely, I will also argue that a certain kind of irregularity is a security asset, not a liability, and governmental structures in place that hinder national uniformity may in fact be powerful protections against disaster, attack and crisis. For instance the lack of uniformity inherent in the American Federal system, while frustrating to efforts at national interoperability, may contribute significantly to American security by spreading out risks, creating a network of federal and concurrent powers and capabilities.

To adequately assess this problem I will consider the nature of unbounded risks and enduring uncertainty, evaluating the security response to each. Ultimately, I will propose a revised approach to theory and doctrine that develops new capacity for managing worst-case possibilities.

C. LITERATURE REVIEW

This summary of research reviews major contributions to understanding the way homeland security has responded to the unknown. This review considered literature on the concept of providing domestic security against mercurial threats and apocalyptic possibilities. There is a growing body of academic literature forwarding the perception that the modern era is one dominated by pervasive security uncertainties and unpredictable catastrophes: in short, the idea that we occupy an era of insecurity. Equally, there is a literature that responds to and tempers or counters this view in multiple ways. The approach to this research has been to understand the major statements of what might broadly be called cultural theory within the context of security. As such, this literature review is broad. The research conducted in support of this review considered legislation, policy, operational doctrine and security theory, in particular since the attacks of September 11, 2001 (9/11). It also considers relevant political and cultural theory relevant to security, as well as important cultural precursors in the form of eschatological myths, and differing approaches to the idea of tragedy and the monstrous. Such literary examples are not presented simply as invocations of poetry or imagination, but to augment the way homeland security professionals might think about the unknown, and to widen our view by considering how others have faced the same problem.

Literature in these areas is primarily qualitative. Where studies are quantitative, as in the actuarial and mathematical evaluation of complex risk, the main interest in this literature review has been the qualitative responses and policy arguments stemming from such probabilistic data, not the data themselves. Additionally, in looking outside strictly security-focused literature, this research considered ways in which navigational science, anthropology and natural science combined with the explanatory and artistic impulses of mapmakers to produce objects that can inform the viewer about the limits of knowledge and the potential dangers of the unknown.

Security theories considered include attempts to formally define and analyze catastrophe, evaluate the idea of a society living with catastrophic possibilities, and establish new methods of responding to security unknowns. Of particular interest is the notion of "worst cases," and literature exists on both the utility of worst-case thinking and its shortcomings in both public opinion and public policy.

This literature review partitions research results into three broad thematic categories: Unbounded Risks (uncertainty and possibility), Unconscionable Maps (our current response to enduring insecurity), and Unseen Doctrine (proposed tools for managing unbounded risks):

- Unbounded Risks: Security risks increasingly defy our ability to control, prevent or compensate the losses associated with them.
- Unconscionable Maps: The dominant mode of current security theory, doctrine, and practice pursues unattainable degrees of knowledge, control of crisis and uniformity in operations.
- Unseen Doctrine: There is significant and under-appreciated literature which should serve to renovate our response to unbounded risk by emphasizing irregularity, modularity, and improvisation.

1. Unbounded Risks

HC SVNT DRACONES

—Inscription from the Hunt-Lennox Globe, 1510[10]

First, things that have never happened before happen all the time in history.

—Scott Sagan[11]

The idea of confronting and securing society against the unknown does not begin with homeland security, or the attacks of 9/11. Around 1539, Swedish cartographer and church historian Olaus Magnus printed his *Carta Marina*, or "map of the seas."[12] Adorning the margins of the known world, Magnus included iconic depictions of sea monsters, coiled and dangerous in the vast deeps of the ocean. It is easy to think of early cartographers as superstitiously filling in the margins of their maps with the horrors of fantasy. But, cartographic experts argue that while the depictions of dragons appear to be mere whimsy to the modern eye, they were based on reliable, academic accounts and scientific literature of the day.[13] They were the best expressions available concerning the many unknowns and dangers of the open sea. Moving into the 18th century, depictions of sea monsters were largely supplanted by depictions of ships—indicating a shift from regarding the sea as unknown and monstrous, to viewing it as a resource to be exploited. In at least one Portuguese map of the 18th century, the king is depicted astride a tamed sea monster.

[10] Meeri Kim, "Oldest Globe to Depict the New World May Have Been Discovered," *The Washington Post*, August 19, 2013.

[11] Scott Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1995), 12.

[12] *Olaus Magnus, Carta Marina et Descriptio Septemtrionalium Terrarum Ac Mirabilium Rerum in Eis Contentarum, Diligentissime Elaborata Annon Domini 1539 Veneciis Liberalitate Reverendissimi Domini Ieronimi Quirini* [A Marine map and Description of the Northern Lands and of their Marvels, most carefully drawn up at Venice in the year 1539 through the generous assistance of the Most Honourable Lord and Patriarch Hieronymo Quirino] (Venice, Italy: 1532).

[13] Chet Van Duzer, *Sea Monsters on Medieval and Renaissance Maps* (British Library, 2013), 12.

Many later maps continued this trend, demonstrating a cartographic response to the limitations of certainty in as yet unknown worlds.[14]

The Latin phrase HC SVNT DRACONES, meaning “here be dragons,” appears on several globes and maps, while TERRA INCOGNITA adorns others, often accompanied by depictions of dangerous and (to the modern eye) fantastical creatures. Map expert Chet Van Duzer and others have argued that this may serve a similar purpose of explanation and warning in spaces unknown.[15]

Beyond cartographic concerns, early explorers confronted persistent myths among their crew concerning the dangers and unknown perils of uncharted waters. Early Portuguese explorers’ log books recount the challenge of sailing beyond navigational charts with crews who believed that monstrous magic lay there.[16]

Security theorists in a variety of applications have picked up this notion of undiscovered country, and operating beyond the boundaries of the familiar. Patrick Lagadec has written extensively on the role of crisis managers and responders in “sense making” within the unknowns generated by crisis situations.[17] Likewise Claudia Aradua and Rens Van Munster have argued that catastrophe by definition represents a rupture with the normal that brings governmental structures to the very limits of their knowledge and ability to respond.[18] These authors use the phrase as more than metaphor–emphasizing the strategic and governmental mechanisms necessary for navigating in unfamiliar places.

[14] Paulo Forlani, *Vniversale Descrittione Di Tvtta La Terra Conoscivta Fin Qvi* [a map of the world from 1565] (1565). There are many examples of maps that contain labels of terra incognita, but Forlani’s map in particular is a powerful example of the cartographic response to limited certainty.

[15] Van Duzer, *Sea Monsters on Medieval and Renaissance Maps*, 12.

[16] Gomes Eannes de Zurara, *The Chronicle of the Discovery and Conquest of Guinea Vol. II*, translated by Charles Raymond Beazley and Edgar Prestage (New York, NY: Burt Franklin 1899), 313.

[17] Patrick Lagadec, “Leadership in Terra Incognita – Mapping the Way for Senior Executives,” *Crisis Response Journal* 6, no. 3 (2010).

[18] Claudia Aradau and Rens Van Munster, “Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future,” *European Journal of International Relations* 13, no. 1 (2007): 89–115.

Central to this body of literature is the idea of a security landscape that contains many unknowns and uncertainties. Security specialists have looked to the idea of an unmapped landscape as a way of expressing uncertainties about space and time, and as an expression of the current limitations of knowledge. Likewise they have viewed crisis and catastrophe as unique situations that augment or generate unknown operational landscapes.

His argument echoes that of Ian Hacking, whose 1990 work *The Taming of Chance* argues that the growth of probabilistic thinking in the 19th century eroded the notion of determinism.[19]

Risk is a modern invention. It is variously defined as, "the probability and magnitude of a loss, disaster or other undesirable event," or, "when it is possible, at least in principle, to estimate the likelihood that an event (or set of events) will occur."[20] Contained in definitions of risk is the idea of calculated likelihood, which is born out of probabilistic science. In *Against the Gods*, Peter Bernstein argues that the modern world can be well understood through the story of the birth, growth and dominance of probabilistic thinking, and the calculation of risk.[21] Similarly, in his book *The Taming of Chance*, Ian Hacking has described the invention of risk as a shift out of the world of pure causality. "Causality," says Hacking, "long the bastion of metaphysics, was toppled, or at least tilted: the past does not determine exactly what happens next."[22] Probabilistic thinking changed the relationship that humans had with the future. Whereas in more primitive times, so the thinking goes, the past was the force dominating the present, the concept of probability allowed the future to govern the present. Risk undermined the long held view of causality that dominated Aristotle's *Physics* and critiques of Aristotle in the

[19] Ian Hacking, *The Taming of Chance, Ideas in Context* (New York, NY: Cambridge University Press, 1990), 1.

[20] Douglas Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (New York, NY: John Wiley and Sons, 2009), 8, and Clarke, *Mission Improbable*, 11.

[21] Peter Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York, NY: John Wiley & Sons, 2012), 1.

[22] Hacking, *The Taming of Chance*, vii.

middle ages.[23] Rather than emphasizing the inevitabilities of causation, risk presumed regular, but uncertain elements of chance. To Hacking's thinking, this meant something radically different even than the Enlightenment era pursuit of universal laws of nature, and opened the way for regular, and yet uncertain patterns. Says Hacking, "A space was cleared for chance."[24]

And this concept of chance in turn opened the door for the development of more robust measures of taking and controlling risks. From the beginning, risk was not simply a way of understanding what bad things might happen, but a means of governing decision-making. "Chance" Hacking writes, "made the world seem less capricious: it was legitimated because it brought order out of chaos. The greater the level of indeterminism in our conception of the world and of people, the higher the expected level of control."[25] Hacking's observation may be no less revolutionary, almost paradoxical. Understanding that the future was uncertain—thus unwritten—society had the right to expect greater control over it. Only knowledge sufficient to calculate was wanting.

Risk, then, might be properly conceived of as a means of control based on known probability. It is a wager on the future. As Hacking's title suggests, it is the taming of chance. This makes an exciting prospect. Knowledge of world phenomena could provide sufficient information to make rational assessments about what might occur in the future. This was the origin of systems of credit, insurance, and a dramatic shift in society's relationship with uncertainty. And this relationship with uncertainty is central to homeland security doctrine and practice. Risk is an idea in opposition to politics, fear, and mindless security musculature. Risk is synonymous with sobriety. In this frame, and the doctrines that have followed, risk is a tool for ordering security capabilities by a disciplined assessment of the threats they are arrayed against. "The decentralized nature of today's threat," says the DHS *Quadrennial Homeland Security Review*, requires an

[23] Aristotle, *Physics*, translated by Robin Waterfield, and David Bostock (Oxford, UK: Oxford University Press, 1999), and Nicole Oresme, *Le Livre Du Ciel et Du Monde* [book of heaven and the world], translated by A. D. Menut and A. J. Denomy (Madison, WI: University of Wisconsin Press, 1941).

[24] Hacking, *The Taming of Chance*, 1.

[25] Ibid.

emphasis on risk-based security as a means to, "shrink the haystack."[26] Security is no longer a question of the tectonic contests between nation states, but radically decentralized networks, insurgencies, technological and natural hazards. The question of chance and uncertainty is central to the way we must think about security.

In *Normal Accidents*, Charles Perrow observed that modern high-risk technological systems are increasingly complex and tightly coupled.[27] Perrow is careful with his terminology, explaining that complex interactions in a system follow an unexpected sequence and may be invisible, as opposed to linear interactions, which may be complicated, but are discernable and regular. In complexity, one part of a system may interact with another part in a way that was not designed.

In the term "tightly coupled" he is describing the inevitability of sequencing, and the deliberate design of system redundancies. This makes systems more efficient, but it also makes room for catastrophe. The result of these two characteristics is that seemingly small mistakes can be amplified as their interdependencies are revealed. Increasingly dense infrastructure and urban areas allows the impact of seemingly small mistakes to be amplified across a system. It is the nature of complex, tightly coupled, socio-technical systems however that such "normal accidents" do not remain small, or escape notice. Magnified across a system, they can produce catastrophic results. The hidden interactions of complexity are revealed in catastrophe.

Perrow generalized normal accident theory in *The Next Catastrophe*, which combined the principles of Normal Accidents with the imagination of Clarke's *Worst Cases*. In examining the larger scale social arrangements in the United States particularly, Perrow perceives an increasingly tightly coupled society.[28] The tendency in everything from infrastructure to the construction of housing is towards higher density, more

[26] Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: DHS, 2014), 35.

[27] Charles Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton Paperbacks (Princeton, NJ: Princeton University Press, 1984).

[28] Charles Perrow, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (Princeton, NJ: Princeton University Press, 2011).

centralized control, and tight coupling. Perrow highlights that the explosion of a single chlorine tanker outside of Los Angeles could poison 4 million people.[29] Power grids, transportation routes, and perhaps even governmental institutions indicate increased consolidation and seamlessness, meaning the modes of failure are increasingly drastic, such as the massive power outage of 2003 that affected upwards of 50 million people across the east coast, and was caused by a sagging power line somewhere in Ohio.[30]

Writing on the nature of modern insecurity and globalization, Christopher Coker argues that there has been a shift in language, or the way in which we talk and think about the threat of terrorism versus the known enemies of the cold war. “The language of danger,” says Coker, “has now turned into the language of risk.”[31] Security policy makers and professions now face the shift from a clear and present nation state threat, to a networked, chimerical terrorist threat, and the ideas of this shift have generated a significant body of literature. The attacks of 9/11 in particular forced a reexamination of security postures not focused on defeating or subverting a discrete threat, but protecting against omnipresent, unpredictable, and not wholly eradicable risks.[32] Amy Kaplan, Michael Barkun, and Mikkel Rasmussen have each written critically that the implication of omnipresent risk sets limitations on the amount of security that a government can

[29] Ibid., 188.

[30] National Public Radio, “How a massive power outage sent people dancing in the street,” August, 2013. Accessed July 1, 2015. http://www.npr.org/2013/08/11/210700217/how-a-massive-power-outage-sent-people-dancing-in-the-street.

[31] Christopher Coker, *Globalization and Insecurity in the Twenty-First Century* (Oxford, UK: Oxford University Press for the International Institute for Strategic Studies, 2002), 60.

[32] Mikkel Vedby Rasmussen, “‘It Sounds Like a Riddle’: Security Studies, the War on Terror and Risk,” *Millennium - Journal of International Studies* 33, no. 2 (March 1, 2004): 381–95, and Michael Barkun. “Defending Against the Apocalypse: The Limits of Homeland Security,” *Policy Options*, September 2002.

possibly provide.[33] Within this context, these authors, especially Kaplan, have hinted that the notion of "homeland security" contains an element of insecurity as well.

If Pre-modern dangers were attributed to gods and monsters, German sociologist Ulrich Beck sees risk is an essentially modern concept—"a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself."[34] Beck explains the societal relationship with risk this way:

> The concept of risk reverses the relationship of past, present and future. The past loses its power to determine the present. Its place as the cause of present-day experience and action is taken by the future, that is to say, something non-existent, constructed and fictitious. We are discussing and arguing about something that is not the case, but could happen if we continue to steer the same course have been.[35]

According to Beck, modern risks create a rupture in this relationship with the future. In *Risk Society,* Beck examined the way that the catastrophic impacts of modern risks are curiously separated from their causes. Modern societies have become victims of their own successes as advances in technology result in catastrophic potential damage e.g., nuclear accidents or environmental risks.[36] More recently, Beck addressed the attacks of 9/11 as a symptom and exemplar of the idea of a "risk society." Beck argues that the losses resulting from terrorism (and the impending catastrophes of environmental and technological crises) are impossible to compensate, defy prediction, and thus defy the actuarial and insurance basis of our society. They defy probabilities, and represent, if not increased risk, then what he calls unbounded risk. Beck describes modern risks (technological risk, terrorism etc.) as de-bounded in terms of social, temporal and spatial

[33] Amy Kaplan, "Homeland Insecurities: Some Reflections on Language and Space," *Radical History Review* 85, no. 1 (2003): 82–93, and Michael Barkun, "Defending Against the Apocalypse: The Limits of Homeland Security." *Policy Options,* September 2002, and Mikkel Vedby Rasmussen, "'It Sounds Like a Riddle': Security Studies, the War on Terror and Risk," *Millennium – Journal of International Studies* 33, no. 2 (March 1, 2004): 381–95.

[34] Ulrich Beck, *Risk Society: Towards a New Modernity* (Thousand Oaks, CA: SAGE, 1992), 21.

[35] Barbara Adam, Ulrich Beck, and Joost Van Loon, *The Risk Society and Beyond: Critical Issues for Social Theory* (London, UK: SAGE, 2000), 214.

[36] Ulrich Beck, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

attributes.[37] Where scarcity disproportionately affected the poor in pre-industrial society, modern risks have the potential to leap across political boundaries, and endanger us democratically. Says Beck, “poverty is hierarchic, smog is democratic.”[38] In contrast to the knowable world of probabilities, a “risk society” is shaped by omnipresent, delocalized, incalculable, and non-compensable dangers. This body of work has proven to be a dominant sociological view of what societies do when confronted with the knowledge that they cannot calculate a risk. Terrorist threats target society’s vulnerabilities, replacing chance and accident with malevolence. This creates a troubling rupture in our relationship with risks. And Beck argues that the risk society challenges the idea that liberal nation states can be responsible for providing security for their citizens.[39] The costs of the Chernobyl disaster now impact children who were not even born yet in 1986, and it will impact their children.[40]

The style of thinking about the unthinkable, and pondering the impossible that came with security analysis against nuclear threats has a great deal in common with the conjectural, apocalyptic imagination that informs worst-case scenario planning, and precautionary security measures.[41] And yet surprise endures. Fukishima, Ebola, Hurricane Katrina, each educate us about ourselves. They lay bare the available tools for responding to manifested impossibilities beyond maps and plans. They are instructive for understanding how security organizations respond to the unknown, how they frame it, live with, and feign control over it.[42]

[37] Ulrich Beck, “The Terrorist Threat World Risk Society Revisited,” *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[38] Beck, *Risk Society*, 36.

[39] Ulrich Beck, “Living in the World Risk Society,” *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

[40] Henry Fountain, “Chernobyl: Capping a Catastrophe,” *The New York Times*, April 27, 2014.

[41] Herman Kahn, *Thinking about the Unthinkable* (New York, NY: Horizon Press, 1962), 86.

[42] Ulrich Beck, “The Terrorist Threat World Risk Society Revisited,” *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55. Here Beck claims, “So the hidden central issue in world risk society is how to feign control over the uncontrollable.”

But this view is not universally agreeable. Richard Ericson and Aaron Doyle have disputed Beck's notion that terrorist threats are either incalculable or non-compensable. They argue that the combination of government and private sector capabilities established under the Terrorism Risk Insurance Act (TRIA) has opened up mechanisms for the private sector to insure against catastrophic terrorism losses.[43] This argument asserts that there can be a response both from private industry and government to maintain control over the complex (though not, in this argument, impossibly unpredictable) threat of terrorism. Claudia Aradau and Rens Van Munster share this view, and further claim that even the unknown and uncontrollable may be subject to some of the same principles that inform insurance of complex risks.[44] Where Beck sees the liberal nation state undermined by risk, Ericson and Doyle see it reinforced.

In this thesis, I consider threat and catastrophe as exemplars of unbounded risk. For this reason, they bear defining.

(1) Threat

I consider "threat" both in terms of the way it is used in intelligence doctrine, and in terms of the sense of danger and uncertainty that are contained in the word "threat." In the context of weapons of mass destruction, the FBI has a, "formalized process to assess a potential threat in the field, called the threat credibility evaluation (TCE) process," used to align operational decisions to the assessed character of threat.[45] In each case, assessment provides an analytic certification of danger. Threat is inseparable from the regimes of analysis that perceive and consider it. In the national security context, it is the

[43] Richard Ericson and Aaron Doyle, "Catastrophe Risk, Insurance and Terrorism," *Economy and Society* 33, no. 2 (2004): 135–73.

[44] Claudia Aradau and Rens Van Munster, "Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future," *European Journal of International Relations* 13, no. 1 (2007): 89–115.

[45] Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C. October 18 (2011) (statement of Vahid Majidi, Assistant Director, Weapons of Mass Destruction Directorate Federal Bureau of Investigation).

means of determining whether a danger poses a threat. So, in this thesis "threat" includes the uncertainty around possibility.

(2) Catastrophe

Governmental definitions of catastrophe express a continuum. The National Response Framework describes, "incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters."[46] Examining the dimensions of "worst cases," Lee Clarke considers the tendency to think of catastrophe as, "rare, if not unique, and as striking randomly and without warning."[47] The etymology of the word catastrophe, note Claudia Aradau and Rens Van Munster, "(as opposed to disaster, crisis or emergency) hints at this sense of rupture, surprise or novelty," literally a reversal, or overturning.[48] For this thesis I want to settle on the idea that catastrophe contains both the idea of rupture (surprise, breaking the relationship with risk) and of a scale that defies our available tools.

2. Unconscionable Maps

> *In time, those Unconscionable Maps no longer satisfied, and the Cartographers Guilds struck a Map of the Empire whose size was that of the Empire, and which coincided point for point with it. The following Generations, who were not so fond of the Study of Cartography as their Forebears had been, saw that that vast Map was Useless, and not without some Pitilessness was it, that they delivered it up to the Inclemencies of Sun and Winters.*
>
> —Jorge Luis Borges[49]

[46] Department of Homeland Security, *National Response Framework, second edition* (Washington, DC: DHS, May 2013), I.

[47] Lee Clarke, *Worst Cases: Terror and Catastrophe in the Popular Imagination* (Chicago, IL: University of Chicago Press, 2006), 6.

[48] Claudia Aradau and Rens Van Munster, *Politics of Catastrophe: Genealogies of the Unknown* (London, UK: Routledge, 2011), 1.

[49] Jorge Louis Borges, *Jorge Luis Borges, Collected Fictions*, translated by H. Hurley (New York, NY: Penguin Books, 1998), 235.

> *So we now use the country itself, as its own map, and I assure you it does nearly as well.*
>
> —Lewis Carroll[50]

> *Accordingly, the Federal Government will…continue to enhance the ability of…Federal information-sharing resources to produce and share cross-sector, near real-time situational awareness while protecting sensitive information.*
>
> —National Infrastructure Protection Plan, 2013[51]

This thread of literature review considers the ways homeland security professionals have generated maps in response to threats and hazards. In grouping literature beneath this banner I consider the term "maps" broadly to include the expressions and tools that homeland security agencies have developed to represent and respond to danger. Such maps include plans, threat assessments and the doctrines that inform and orient security actions in the context of national preparedness.

The term "securitization" was coined by Barry Buzan as a way of describing the modes of thinking which frame issues within a security context.[52] This is an influential conceptual frame of reference that has supported widely divergent views of the homeland security enterprise—from critiques of the governmental structures in place for security and crisis response, to harsh criticism of governmental, public and media over-emphasizing of low probability security threats, and finally refinements that argue that it is perhaps irresponsible to ignore low probability threats. Securitization is an expression

[50] Lewis Carroll, and Harry Furniss, *Sylvie and Bruno Concluded* (London; New York, NY: Macmillan and Co., 1893), 169.

[51] Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, 2013), 23.

[52] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998), 23.

of the politics of security. For writers examining the way political power structures influence security, the work of Michel Foucault is also influential.[53]

In response to a culture of securitization, John Mueller has sought to assert probabilities back onto public perception, and emphasized that the threat of terrorism is in decline, and that politicians and profiteers continue to exaggerate the threat posed by terrorism.[54] His work argues both that government spending on combatting a relatively minor threat is excessive, and that governmental approaches to addressing terrorism have resulted in a paranoid inflation of the threat, which results in thinking about too many things from a perspective of danger. Mueller's approach is essentially actuarial—considering principally the likelihood of terrorist attacks, and the ways in which societal opinion and response to low probability events may be shaped by a governmental overemphasis on these threats. Conversely Mueller also considers whether a government that worked harder to frame threats in a low-probability context would do more to sway public fears to match fact.[55] Jef Huysman also examines what he terms the "social construction of danger," where societal fears and concerns over terrorism and other security threats are translated into governmental action to provide security.[56]

Research for this literature also considered existing laws, doctrines and national preparedness architectures outlined in the Homeland Security Act of 2002, and the National Preparedness System idea refined under Homeland Security Presidential Directive 8 (HSPD-8), and Presidential Policy Directive 8: National Preparedness (PPD-

[53] Michel Foucault, Michel Senellart, François Ewald, and Alessandro Fontana, *Security, Territory, Population: Lectures at the Collège de France 1977—1978* (New York, NY: Macmillan, 2009).

[54] John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (New York, NY: Free Press, 2006), 6.

[55] John Mueller and Mark Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford, UK: Oxford University Press, USA, 2011), 172.

[56] Jef Huysmans and Anastasia Tsoukala, "Introduction: The Social Construction and Control of Danger in Counterterrorism," *Alternatives: Global, Local, Political* 33 (April 2008).

8).[57] The creation of a Department of Homeland Security (DHS) proposed a series of primary missions for the department, including, "acting as a focal point regarding natural and manmade crises and emergency planning."[58] HSPD-8 and PPD-8 directed the construction of a National Preparedness System. The National Preparedness architectures within the system now include five mission areas of Prevention, Protection, Mitigation, Response and Recovery, and establish a complex of Federal Interagency Operational Plans for each mission. Together, the production of these documents pursuant to PPD-8 served as a means of organizing the capabilities of the Federal Government to anticipate, and manage crisis and catastrophe. The responsibilities of the DHS Secretary laid out in the Homeland Security Act of 2002 also include the development of a National Incident Management System.[59] The development of this system was generated in part due to the challenges of interoperability and coordination exhibited in the response to the attacks of 9/11. And the challenge of executing this task has generated extensive public and private sector doctrines, plans, and supporting literature.

The Homeland Security Act of 2002 required, "consolidating existing Federal Government emergency response plans into a single, coordinated national response plan."[60] Among the many challenges implicit in this charge was to reconcile different methodologies for conducting incident planning.

The prevalence of scenario-based planning in the civilian sphere owes a great deal to Herman Kahn. Working for RAND Corporation following World War II, he pioneered

[57] White House, *Homeland Security Presidential Directive (HSPD) 8, National Preparedness* (Washington, DC: White House, December 2003), and White House, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: March 30, 2011).

[58] 107th Congress. *To Establish the Department of Homeland Security, and for Other Purposes.* Vol. 116 STAT. 2135, 2002. While the Homeland Security Act identifies seven primary missions, including this statement of all-hazards responsibilities, DHS doctrine often claims that the primary mission of the Department is managing terrorism. For an example of this unsubstantiated claim, see Department of Homeland Security, *The National Prevention Framework* (Washington, DC: DHS, May 2013).

[59] Ibid.

[60] Ibid.

the application of military war game models to domestic security planning.[61] Scenario planning—a term meant to invoke Hollywood film scenes of imagined possibilities—focused resources and operational plans around the potential impacts of plausible enemy actions. Perhaps the conjecture and imagination necessary to confront evolving risks are to be routinized through the development of such scenarios. Scenarios, like risk, consider the past, evaluate the present, and propose a possible future and there is literature to suggest that scenarios can serve as "strategic conversation" that allows organizations to consider and adapt to potential outcomes.[62] While an immensely influential planning and decision-making model, scenario-based planning is a troubled concept within national preparedness. For a homeland security enterprise challenged with facing multiplicity of risks with limited resources, and organizing effort across a wide range of Federal and other public sector entities, capabilities-based planning (also adapted from Department of Defense (DOD) models) is now the prevalent model for developing plans.[63] Capabilities-based within the national preparedness system is defined as, "Planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice."[64] The essential distinction between these two models of planning is that while scenario-based planning optimizes decisions upon considering plausible futures, capabilities-based planning is properly the development of diverse capabilities and detailed organizational knowledge. In practice however, scenario-based methods continue to influence the development of national capabilities assessments, and plans—as plans within the national planning system rely on scenarios to identify capabilities in hazard specific plans.[65] The

[61] Herman Kahn, *On Escalation: Metaphors and Scenarios,* Hudson Institute Series on National Security and International Order (Piscataway, NJ: Transaction Publishers, 2009), 39.

[62] Kees van der Heijden, *Scenarios: The Art of Strategic Conversation* (New York, NY: John Wiley & Sons, 2011), chapter 8.

[63] Sharon Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs* 1, Article 2 (August 2005).

[64] Federal Emergency Management Agency, *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101* (Washington, DC: FEMA, November 2010), B-2.

[65] Federal Emergency Management Agency, *Nuclear/Radiological Incident Annex* (Washington, DC: FEMA, 2008).

principal challenge of planning systems is to develop capabilities and coordination mechanisms that allow homeland security organizations to respond to contingencies. But faced with a complex array of dangers, the state of planning relies on a combination of scenario and capabilities-based approaches designed to prepare organizations for the increasingly complex list of possible futures.

Lee Clarke describes the way that, "to make a plan is to claim expertise," and, "since claims to expertise are always claims that somebody should be left out of the decision loop, planning is deeply, unavoidably political."[66] Both scenario planning and capabilities-based planning are subject to this political character, and the way in which homeland security organizations plan ends up reflecting their beliefs and claims about specific hazards and organizational capabilities.

When security organizations must act, the organizational arrangements and doctrines in place face similar challenges. The Homeland Security Act further required, "building a comprehensive national incident management system with Federal, State, and local government personnel, agencies, and authorities, to respond to such attacks and disasters."[67] The corresponding National Incident Management System (NIMS) doctrine is developed and maintained by the Federal Emergency Management Agency (FEMA), and encompasses the Incident Command System (ICS), which has emerged as the national doctrine for incident management.[68]

First published in February of 2003, Homeland Security Presidential Directive 5 (HSPD-5) addressed the management of domestic incidents. Its purpose was succinct:

[66] Clarke, *Mission Improbable*, 13.

[67] 107th Congress, To Establish the Department of Homeland Security, and for Other Purposes, Vol. 116 STAT. 2135, 2002.

[68] Federal Emergency Management Agency, *National Incident Management System* (Washington, DC: FEMA, December 2008).

> To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.[69]

HSPD-5 directed the adoption of the NIMS by all Federal agencies, and made NIMS a requirement for the receipt of Federal preparedness grants and contracts. By tying preparedness grant funding to the implementation of NIMS among grantees, FEMA commenced a disciplined shift toward, "institutionalizing the use of ICS, across the entire response system" including non-federal responders.[70] Within the NIMS document, FEMA included the ICS as the, "standardized incident organizational structure for the management of all incidents."[71] Likewise, the 9/11 Commission Report recommended the adoption of ICS to, "enhance command, control and communications capabilities."[72]

Much like the planning systems in use, NIMS and ICS are inherited doctrines. Deadly and destructive wildfires in 1970 illustrated the enormous challenges around interagency coordination and communications for responding to complex wildfires with disparate resources. As a result, Congress, "mandated that the U.S. Forest Service design a system that would 'make a quantum jump in the capabilities of Southern California wildland fire protection agencies to effectively coordinate interagency action and to allocate suppression resources in dynamic, multiple-fire situations.'"[73] At root, NIMS and ICS are management systems designed to balance standardization and flexibility. Both confront the enormous challenge of how best to permit different organizations to jointly address the complexity of incidents. And the sustained effort to nationalize the standardized adoption of NIMS is underscored by the relatively long history of the organizational models and planning processes instantiated in ICS.

[69] White House, *Homeland Security Presidential Directive 5: Management of Domestic Incidents* (Washington, DC: February 28, 2003).

[70] "New Position Paper on National Incident Management System (NIMS) Incident Command System (ICS) - Homeland Security Digital Library Blog." Accessed April 16, 2015.

[71] Ibid.

[72] Ibid.

[73] Ibid.

However, writing in 2013, Cynthia Renaud argued for a crucial limitation to the structures of incident command outlined in the NIMS doctrine. The relevance and usefulness of command and control architectures, especially the ICS that is part of NIMS may, according to Renaud, effectively have a lower bound. In the initial moments following incidents, or at a highly localized level, the prefabrication of the ICS system may not lend itself well to the undiscovered and ill-defined parameters of an incident.[74] Organizational studies conducted of urban search and rescue teams using the ICS model similarly have concluded that, "ICS does not create a universally applicable bureaucratic organization among responders but rather is a mechanism for inter-organizational coordination designed to impose order on certain dimensions of the chaotic organizational environments of disasters."[75] In other words, rather than creating a universally adoptable system, ICS is a means for organizations to work together, and it functions by providing an organizational illusion of orderliness to what is, and perhaps remains, chaotic and complex.

If ICS possesses such a "lower bound" of utility, others have argued that it may also be subject to an "upper bound" where incidents approach such organic complexity that emergent organizations produce greater effects than command and control models.[76] The enormous complexity of interacting state, local and federal authorities and catastrophic dangers puts additional strain on organizational arrangements within the command and control model of ICS.[77] This in turn highlights the way in which the federalism model of American government can combine with national policy, doctrine

[74] Cynthia Renaud, "The Missing Piece of NIMS: Teaching Incident Commanders How to Function in the Edge of Chaos," *Homeland Security Affairs* 8, Article 8 (June 2012).

[75] Dick Buck, Joseph E. Trainor, and Benigno E. Aguirre, "A critical evaluation of the incident command system and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006).

[76] Robert Owen Gardner, "The Emergent Organization: Improvisation and Order in Gulf Coast Disaster Relief," *Symbolic Interaction* 36, no. 3 (August 2013): 237–60.

[77] Thomas A. Birkland and Sarah E. DeYoung, "Emergency Response, Doctrinal Confusion, and Federalism in the Deepwater Horizon Oil Spill," *Publius: The Journal of Federalism* 41, no. 3 (July 1, 2011): 471–93.

and law to erode the necessary conditions in which command and control might flourish.[78]

Perhaps surprisingly, military doctrines of command and control have begun to experience significant evolutions toward greater decentralization and field level improvisation in response to volatile and evolving counterinsurgency missions.[79]

Even in a state of such disciplined readiness, the unthinkable continues to happen to us. After action reporting in the wake of security crises further reveals aspirations to control, knowledge and uniformity within response operational arrangements and doctrines. The Navy report on the 2013 Navy Yard shooting in Washington, DC concluded that local and federal law enforcement failed to share key pieces of information such as the availability of live video within the building.[80]

The final thread of this literature review, however, may temper the creation of unconscionable maps. "Unseen doctrine" is a term that describes a set of theory, capability, and practice that may significantly renovate the security response to catastrophe and threat.

3. Unseen Doctrine

> *The landscapes I have in mind are not part of the psychic sense, nor are they part of the Unconscious. They belong to the world that lies, visibly, about us. They are unseen merely because they are not perceived; only in that way can they be regarded as invisible.*
>
> —Paul Nash[81]

[78] Andrew C. Teeter, "On A Clear Day, You Can See ICS: The Dying Art Of Incident Command And The Normal Accident Of NIMS—A Policy Analysis" (master's thesis, Naval Postgraduate School. March 2013).

[79] Martin E. Dempsey/General, U.S. Army/Chairman of the Joint Chiefs of Staff, *Mission Command: White Paper* (Washington, DC: April 3, 2012).

[80] Department of the Navy, *Report of the Investigation Into the Fatal Shooting Incident at the Washington Navy Yard on September 16, 2013* (Washington, DC: November 8, 2013).

[81] Robert Macfarlane, *The Wild Places* (New York, NY: Penguin, 2008), 225.

The poetic Edda is an ancient collection of Norse mythology—including an account of Ragnarok, the, "traumatic climax" and, "great global catastrophe of the future" resulting in a new and better world.[82] This is a theme echoed in literature, including the provocative poetry of *Beowulf* and subsequent studies in the nature of tragedy and terror in human experience.[83]

There is a parallel literature in the realm of national preparedness built on the exploration of worst-case scenarios. Worst-case thinking, according to sociologist Lee Clarke can serve a utilitarian purpose, but is also subject to distortion.[84] As argued by Clarke, regulators and security professionals must consider low probability events such as airplane crashes despite their likelihood, and that security agencies need to augment probabilistic thinking with possibilistic—e.g., investigating an airplane crash even though the probabilities of planes crashing are already sufficiently low. But possibilistic thinking, says Clarke, can be misused. Fear of worst cases can justify invasions of privacy or abandonment of risk-based decision-making. The value of plans, however, which articulate government responses to highly complex, catastrophic or uncertain incidents is twofold—it both encourages creative and possibilistic thinking in responders, and assures the public that the government is ready to respond and protect against dangers.[85] But, says Clarke, these are not necessarily cynical documents. The organizations the produce them can be just as susceptible to the rhetorical qualities of this type of plan. In cases where planners have sufficient information to transform uncertainties into manageable risks, plans may well govern the actions that organizations will take. But where this level of rationality is not attainable, plans may become fantasy documents. Clarke calls for a tempered approach to catastrophism, and for organizational humility in assessing the ability to manage ubiquitous worst cases. In his estimation, the

[82] Olive Bray, trans., *The Elder or Poetic Edda - Commonly Known as Saemon's Edda* (London, UK: King's Weighouse Rooms), 1908, 10.

[83] Terry Eagleton, *Sweet Violence: The Idea of the Tragic* (New York, NY: Wiley, 2009), xv.

[84] Clarke, *Worst Cases*, 177.

[85] Clarke, *Mission Improbable*, 16.

Cassandra impulse of fear and dread has in fact grown too rare. American society has difficulty accepting loss or disaster that cannot be compensated. Meanwhile disasters continue to exceed our capacities.

Man-eating predators have occupied, according to David Quammen, a unique and fearful place in human cultural symbols, myths and social structures.[86] From the “crooked serpent” of the biblical leviathan to ancient tiger and lion symbolism, Quammen argues that these “monsters of god” served as fearful symbols of strength as well as human mortality. There is a parallel here with Clarke’s measured catastrophism, in understanding how human culture has responded to the enduring presence of possible danger.

Similarly, Paul Slovic has worked extensively to examine the way in which the perception of risk can define our reactions, and may even present a danger by itself.[87] Considering how people respond based on feelings rather than simply data, Slovic has emphasized the social and cultural amplifications of risk.

Nassim Taleb’s *The Black Swan* argues that unpredictable, high consequence events have a disproportionate influence on human affairs.[88] And, he argues, this severely erodes the idea of risk predictability or large-scale risk management. This book is concerned with what Taleb argues is a human blindness to randomness and large deviations. In Taleb’s thinking, what is unknown becomes more important than what is known. It is a book about uncertainty, and Taleb argues that it is important to study rare and extreme events as a means to explain more common events—not the reverse. He argues that our current approach, which is to rule out less common events and focus on “normal” ones, neglects so called “outliers” as aberrations. But, when he considers the

[86] David Quammen, *Monster of God: The Man-Eating Predator in the Jungles of History and the Mind* (New York, NY: W.W. Norton & Company, 2004).

[87] Paul Slovic, *The Perception of Risk* (London, UK: Earthscan Publications, 2000).

[88] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York, NY: Random House Publishing Group, 2007).

disproportionate impact of outlier events, the problem deepens. Taleb argues eloquently for the futility of predictive analysis of markets—and almost everything else.

Taleb's views are not universally shared. Swiss risk expert Didier Sornette has proposed a countervailing theory, reframing Taleb's notion of "gray swans" (significant incidents which, unlike black swans may be predictable) as Dragon Kings.[89] As Sornette contends, crises are potentially predictable, if extremely complex, through the application of models for power laws (the functional relationships in probability between lower and higher impact incidents). Sornette has attempted to lay the groundwork for predicting catastrophes including earthquakes and market crashes. The as yet unverified hope for Sornette's work is the prediction of crisis, and a better calibration of response to crisis, along with the ability to avoid it. Black Swans and Dragon Kings represent two contemporary views of the same issue—the limitations of certainty and the way in which security professionals should respond to it.

Our current ways of thinking about uncertainty and risk have led to the dominance of what Cass Sunstein describes as the "precautionary principle." This principle is broadly the idea that it is better to be safe than to be sorry—which can translate into a bias for or against taking action. Sunstein argues that precaution, if taken too strongly, can result in paralysis as the risk of taking action and not taking action each produce subsequent risks.[90] Precaution as the dominant mode of regulation and security policy, according to Sunstein, imprisons decision makers between impossible risks on all sides of pressing social issues.[91] Sunstein makes a distinction between risk and uncertainty, examining the precautionary principle against what he calls the "Maximin" principle. In this paradigm, when regulators are unable to assign probabilities to uncertain outcomes, they must instead choose the policy with the best worst-case outcome.[92]

[89] Didier Sornette, "Dragon-Kings, Black Swans and the Prediction of Crises," *International Journal of Terraspace Engineering*, 2 (1), 1-18 (2009).

[90] Cass Sunstein, "The Paralyzing Principle," *Regulation* 25, no. 4 (Winter 2002/2003): 32.

[91] Cass Sunstein, *Laws of Fear: Beyond the Precautionary Principle, John Robert Seeley Lectures* (New York, NY: Cambridge University Press, 2005).

[92] Ibid.

Sunstein proposes balancing precaution against attention to probabilities. In situations of unknown probabilities and incalculable costs, we need to adopt an "anti-catastrophe principle"—taking action to avoid the worst-case outcome even in the absence of confirming fact.[93] The same principle may perhaps be applied to the development of regulatory policy, or tools of homeland security governance. Sunstein's work serves a regulatory primer, outlining a set of principles that may serve as a guide for policy makers in navigating their responsibilities to both probability and precaution. In considering indefinite probabilities and measureless damages, we may need to modify our approach to scenario design, operational planning, policy and operational implementation to pursue the best worst case, rather than invest in preventing all possible cases.

The literature of attempting to counter unbounded and extreme events is equally rich. Charles Perrow has argued that one solution to the "normal accidents" of tightly coupled complex systems and the humans that interact with them is to pursue "modularity."[94] This idea of modularity means a reduction in the concentration of vulnerability, such as the grouping of populations in high-risk areas, or the reliance on concentrated infrastructure arrangements such as the prevalence of extra-high voltage transformers in the electrical grid. Distribution of risk is a common theme in resilience literature, often referred to as "semi-autonomy" and has been augmented by Nassim Taleb's notion of what he calls "antifragile" systems.[95] Fragile things, according to Taleb, like teacups or poorly designed buildings, do not like volatility. Robust things, like diamonds or hardened structures do not particularly care—up to a defined tolerance. Antifragile systems are responsive to trial and error, flexible, adaptable, decentralized, and may even require volatility to flourish. In antifragile systems, all mistakes are good mistakes, because they spread and decentralize error, and therefore impacts. The principle

[93] Ibid.

[94] Charles Perrow, "Complexity, Catastrophe, and Modularity," *Sociological Inquiry* 78, no. 2 (May 2008): 162–73.

[95] Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder, Incerto Series* (New York, NY: Random House, 2012).

response to uncertainty here is decentralization and resisting the tendency to concentrate dependencies.

For the responder who must react to uncertain and uncontrollable incidents, the literature also provides some unusual refinements to current thinking. In 1957, Omar Khayam Moore published "Divination—A New Perspective" in The American Anthropologist.[96] His paper forwards the startling argument that magical practices in some cultures—traditionally dismissed by anthropologists as non-effectual—may actually produce their desired effect. Not, he argues, through actual magic, but by serving to randomize human behavior in relation to prey (such as the caribou) that responds to and tries to anticipate the actions of hunters, and by providing a sense of certainty in unpredictable situations. In view here is the possibility that developing systems of randomization may help responders address unpredictable enemies and threats.

A close corollary to this notion Patrick Lagadec's insistence on responder sensitivity to absurd rather than weak signals.[97] Arguing that catastrophe and crisis push responders into unfamiliar territory, the modern responder must develop and adopt a comfort with recognizing and exploring the unknown without the expectation of being able to revert to familiar practices or rote solutions.

Patrick Lagadec advocates and trains crisis professionals in the use of a rapid reflection force (RRF).[98] Responders to modern crisis, argues Lagadec, must develop expect that it will not conform to procedures, plans, or even the domains constructed for managing disaster. The RRF is a notional interdisciplinary body not tied to the direct function of response, but tasked with anticipating the weak, even absurd signals that characterize modern crisis. Incorporating an RRF as part of a response organization is meant to provide a level of reflection and anticipation beyond the execution of immediate

[96] Omar Khayam Moore, "Divination—A New Perspective," *American Anthropologist, New Series*, 59, no. 1 (February 1, 1957): 69–74.

[97] Patrick Lagadec, "Leadership in Terra Incognita—Mapping the Way for Senior Executives," *Crisis Response Journal* 6, no. 3 (2010).

[98] Patrick Lagadec, "A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice," *Review of Policy Research* 26, no. 4 (2009): 473–86.

tasks. As Nassim Taleb has argued that what we do not know is far more dangerous than what we do know, Lagadec's exploratory frame of thinking is intended as tool for navigating a universe of increasing and omnipresent uncertainty.[99] For Lagadec, this means being comfortable with deviating from procedure. As situations refuse to conform to rote procedure, responders should be comfortable exploring and experimenting within response to crisis.

D. RESEARCH DESIGN

Studying the borderland where homeland security reach exceeds grasp, this research seeks to understand and reform the way we conceptualize and manage unmapped security problems at the edge of our understanding. Such problems include the unpredictable possibilities of cataclysmic terrorism or catastrophes of staggering complexity or unique surprise.

1. Selection

Within the homeland security enterprise, I have circumscribed this study by focusing on the concept of national preparedness. Borrowing from the evolving concept of a national preparedness system initiated in HSPD-8, and revised under PPD-8, I have narrowed this research and argument to the way in which homeland security theory and practice manages contingency events across multiple missions and disciplines.[100] This has meant excluding a consideration of more persistent issues such as immigration, economic or environmental policy, and fixing on operational concepts and practices.

The concept for this thesis began with studying a renaissance map, and marveling at the depiction of dragons as informed conjecture about unknown places.[101] The process I used to initially scope and select the research object required understanding risk,

[99] Taleb, *The Black Swan*.

[100] White House, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: March 30, 2011).

[101] Van Duzer, *Sea Monsters on Medieval and Renaissance Maps*, 12.

uncertainty and maps (conceptualizations) in homeland security applications. The overlaps and a basic view of this initial literature review are reflected in Figure 1.

2. Limits

This research is an observation and analysis of how unbounded risks influence security theory—including philosophical and epistemological beliefs and assumptions about security. And, when problems defy existing concepts of control, this research considers how current theory and corresponding doctrine and practice fares, and whether refinements may be in order. Second, this research will principally address strategies and doctrinal approaches for governing uncertainty, rather than directly assess crisis decision-making, or social and organizational psychology. Finally, as mentioned above, this study is bounded by an emphasis on national preparedness, to the exclusion of persistent security issues such as immigration or economic policy. Rather, this study relies in part on the concept of national preparedness provided in PPD-8 as a means of building and marshaling capabilities to manage security risks.

3. Data Sources

The data used in this study includes a literature review and primary source documentation in the form of publicly available plans, strategic national risk assessments, doctrinal statements and homeland security laws, regulations and presidential directives.

Additionally, I will consider small-scale case studies that are illustrative of the limitations of procedure, and the advantages and strengths of unconventional, exploratory methods for managing uncertainties.

4. Type and Mode of Analysis

This research follows a qualitative approach, producing a prescriptive set of recommendations based on hermeneutic method.

a. Qualitative Approach

Research will be qualitative, indicating that words, ideas, expressions and concepts of governance are the data under consideration, rather than numbers.

b. Prescriptive Paradigm

In exploring successful possibilities for managing uncharted security landscapes, I hope to provide a set of rules, recommendations or methods.

c. Hermeneutic Method

Hermeneutics is the art and science of interpretation.[102] This thesis is more concerned with what the homeland security enterprise has made of quantitative fact than it is about the facts themselves. As a method, hermeneutics proposes to pierce the divide between art and science, and between science and philosophy.[103] Such an approach is essential for the theoretical territory of this thesis. To study the imaginative and interpretive approaches in place for dealing with elusive security problems requires a means of examining the interstitial space between object (threat and catastrophe) and interpretation (policy, doctrine, conceptual maps and operational plans). This research will follow an inductive method to generate a theory and conceptual framework grounded in systematic analysis and comparison of three main bodies of security literature and cultural criticism: maps, risk and uncertainty.

As a methodology, hermeneutics requires a cyclical, recursive approach to assessment of existing literature, interpretation and conjecture, theory, and argument. The process is designed to ensure logical rigor and broad consideration of existing interpretive frames of policy and practice. Figure 1 provides a further view of the way the speculative hermeneutics provides an analytic approach to comparing and evaluating a plurality of interpretations. As an enterprise made up of diverse disciplines, stakeholders, agencies,

[102] William Saffire, "On Language; Hermen Eutic's Original Intent," *The New York Times*, September 6, 1987, sec. Magazine.

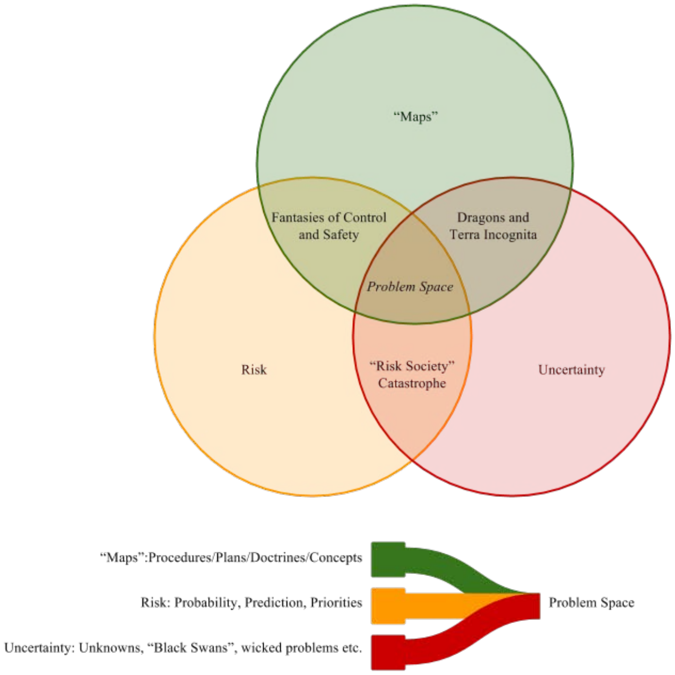
[103] Hugh J. Silverman and Don Ihde, *Hermeneutics and Deconstruction: Selected Studies in Phenomenology and Existential Philosophy* (Albany, NY: State University of New York Press, 1985), 5.

legal authorities, etc., homeland security is not lacking for varied interpretations and views of identical information. For this reason, hermeneutics is an especially apt approach for assessing the uncommon ways in which interpretation of uncertainties has generated explicit and implicit theories in homeland security practice.

Finally, hermeneutics is interpretive in contrast to an inventive approach. The prescriptive paradigm of this thesis will rely on interpretation as a means of providing rigor to theory development, rather than proposing a wholly new or inventive theory.

However, in offering prescriptions, induction does imply a measure of creativity in producing a theory. "The man," says J. Bronowski, "who proposes a theory makes a choice—an imaginative choice which outstrips the facts...every induction is a speculation, and it guesses at a unity which the facts present, but do not strictly imply."[104]

Figure 1. Conceptual Model for Hermeneutic Approach


"Maps"
Fantasies of Control and Safety
Dragons and Terra Incognita
Problem Space
Risk
"Risk Society" Catastrophe
Uncertainty
"Maps":Procedures/Plans/Doctrines/Concepts
Risk: Probability, Prediction, Priorities
Uncertainty: Unknowns, "Black Swans", wicked problems etc.
Problem Space

[104] J. Bronowski, "The Creative Mind," *Scientific American, Art In Science* (New York, NY: Simon and Schuster Inc. 1954).

5. Output

The output of this thesis is a proposed homeland security theory highlighting the problems of unbounded risk, and proposing approaches that refocus the homeland security enterprise away from fantasies of control, and toward disciplined irregularity, exploration, and adaptability.

II. RISK UNBOUND

The last few decades have witnessed an extraordinary development in the sciences and techniques of risk control and crisis management. However, there is a gnawing doubt: what if our points of reference, our capabilities, are no longer good enough?

—Patrick Lagadec[105]

Ai! Ai!
The elements obey me not. I sink
Dizzily down, ever, for ever, down.
And, like a cloud, mine enemy above
Darkens my fall with victory! Ai, Ai!

—Jupiter[106]

In this chapter I will argue that the dangers homeland security agencies confront are increasingly beyond the reach of measures for control. In the first place this is because the character of the risks we face is changing. Secondly, it is because worst cases, not merely probable accidents and disasters, are particularly relevant to domestic security agencies and organizations. Because homeland security organizations lack the ability to select or decline risks the way, for instance, insurance companies might, catastrophe, threat, and concentrated uncertainty dominate their concerns. This presents a challenge to the idea that homeland security programs must be risk-based, because the uncertainty and possibility of such risks strain available risk management tools.

Citing an older maritime edict, 6th century Roman law established, "that if merchandise is thrown overboard to lighten the ship, the loss occasioned for the benefit of all must be made good by the contribution of all."[107] Given uncertainty, this was a

[105] Patrick Lagadec, "Risks and Crises in Terra Incognita," *Paris Tech Review* (October 10, 2010).

[106] Percy Bysshe Shelley, *Prometheus Unbound: A Lyrical Drama in Four Acts* (London, UK: J.M Dent and Company, 1898), Act iii, Scene i.

[107] Justinian, *The Digest of Justinian*, translated by Charles Henry Monro, Edited by William Warwick Buckland (Cambridge, UK: Cambridge University Press, 1909), 385.

means of distributing the loss of cargo between the merchant and the captain. In the intervening centuries, probabilistic and observational science have combined to offer improved means of taking calculated risks. The idea of risk offers something new to this early insurance scheme: control.

Risk, says Ulrich Beck, "inherently contains the concept of control. Pre-modern dangers were attributed to nature, gods and demons. Risk is a modern concept. It presumes decision-making."[108] For a people who have a spent hundreds of years living by the future and organizing so many of our actions based on an ability to rationally anticipate the horizon, there is something traumatic in events that violate our schemes of management. Tragedy, surprise, attack, threat and catastrophe all describe the rupture of a reliable relationship with the future. They are the bubbling up of insecurity.

Presenting this will require a brief explanation of what makes it possible to transform uncertainty into risk and what it means to manage risks that we know enough about to inform rational decisions. But more importantly, I will examine the ways in which contemporary risks violate our ability to manage them. Ulrich Beck argued that "The speeding up of modernization has produced a gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities that we are creating."[109] Homeland security agencies inherit these non-quantifiable insecurities. And the result of this process is a set of modern risks that are, according to Beck, "de-bounded" along spatial, temporal and social dimensions.[110] This in turn causes such risks to defy efforts at risk calculation and control. To Beck's tripartite frame, I

[108] Ulrich Beck, "The Terrorist Threat World Risk Society Revisited," *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[109] Ulrich Beck, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

[110] Ibid.

make a case for a fourth dimension, that of rationality—arguing that the burgeoning hyper-complexity of crises particularly defies our ability to make sense of them.[111]

For homeland security agencies tasked with responsibly adjudicating limited resources to provide against an expanding menu of threats and hazards, this is problematic. Unbounded risk undermines the concept of risk-based security, but it does not undermine the concept of risk or risk management generally. Rather, it describes the relationship that homeland security must develop with risks that are particularly difficult to manage, either because they are highly uncertain or catastrophic. It is precisely the uncertain element, and the catastrophic possibility that is of particular importance to homeland security agencies.

Ultimately, I conclude the homeland security risks are becoming unbound, and the result is a security wilderness, increasingly unresponsive to the measures in place for control.

A. RISK-BASED SECURITY

9/11 was extremely unlikely. The mode of attack was unexpected, and its impact was likely worse than even the attackers intended.[112] The world, and Americans in particular, will confess that its improbability offers no comfort. Terrorism in America remains highly improbable, but disquieting. Averages and aggregates are diminished in the face of cataclysm, just the way that a kidnapped child is an extraordinarily unlikely event, but an unmitigated tragedy for that particular family. Neither the rare earthquake nor the outlier tsunami is tolerated through the comfort of improbability. Rather, they

[111] Erwan Lagadec, "Unconventional Crises, Unconventional Responses: Reforming Leadership in the Age of Catastrophic Crises and Hypercomplexity," *Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies* (Baltimore, MD: Johns Hopkins University, 2007).

[112] Richard Muller, *Physics for Future Presidents: The Science Behind the Headlines* (New York, NY: W.W. Norton & Company, 2008), 28. Echoing the results of the National Institutes for Standards and Technology and FEMA Building Performance Assessment Team investigations into the collapse of the world trade center, Muller notes that the burn rate that generated sufficient heat to melt portions of the steel framing in the building was limited not by the amount of fuel, but by the available oxygen. This, combined with the immense weight of the structure above the impact, resulted in the "pancaking" failure that brought the building down, the same way a soda can is able to support the weight of a person, but collapses when its side is impacted.

dominate our thinking with their horror—perhaps because they are distinct and seem to us unusual. And yet, conscious that security agencies must confront the unthinkable with limited resources, DHS Secretary Michael Chertoff insisted as early as 2005 that, "DHS must base its work on priorities driven by risk."[113] What can he have meant?

Chertoff's admonition contains two ideas. First, managing individual threats and hazards requires the discipline of risk analysis. Second, that we must face a multitude of dynamic threats with limited resources. A risk basis for security actions is both a method for the control and management of individual risks, and a means of being judicious in addressing a multiplicity of risks.

And DHS doctrine provides a framework for how the department is to go about this task, and develop a, "common organizational understanding of and approach to," managing risk.[114] The DHS *Risk Lexicon* defines risk as, "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences," and risk management as the, "process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken."[115] Carrying through on this approach to risk requires homeland security to demonstrate both knowledge and control of risk.

Not surprisingly the DHS annual Financial Report to its oversight and appropriation bodies in Congress for fiscal year 2014 contains more than one hundred references to risk, its management and reduction, and the development of risk-based

[113] Todd Mass, Siobahn O'Neil, and John Rollins, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (CRS Report No. RL33858) (Washington, DC: Congressional Research Service, 2007), Summary, http://www.fas.org/sgp/crs/homesec/RL33858.pdf.

[114] Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, DC: DHS, April 2011).

[115] Department of Homeland Security Risk Steering Committee, *DHS Risk Lexicon 2010 Edition* (Washington, DC: DHS, September 2010).

security measures.[116] Risk management, the taming of chance, is a central figure in the doctrine and program development across a homeland security enterprise increasingly driven to efficiency by oversight and appropriation. From border security programs to Transportation Security Administration (TSA) screening measures, homeland security must, it seems, be risk-based.

Undergirding such insistences on risk is a sophisticated and complex body of analytic science. A common framework for understanding this analysis is to determine the probability of something bad happening (threat), the extent of its damages (consequence), and the measures in place to reduce the impact (vulnerability). Expressed as a formula: Risk = threat x vulnerability x consequence.

This formula has reached totemic proportions, and become a kind of explanatory phenomenon. In it, we find a means for understanding what we want to protect, and how much we are willing spend to protect it.[117] John Mueller has argued that such calculation offers a means of critiquing homeland security spending. Homeland security agencies should, in his view, demonstrate that the cost of security measures do not outweigh the benefits.[118] Mueller summarizes the method this way:

> Thus, for a successful attack in which the enhanced security cost is $75 billion, losses sustained are a very high $100 million, and the reduction in risk is .45, the probability of a successful attack would need to be at least
>
> (probability of a successful attack) > $75 billion/[$100 million x .45] = 1,667 attacks per year[119]

Elsewhere, Mueller points out that in order to break even on counterterrorism spending, from a cost/benefit standpoint the United States would need to be experiencing

[116] Department of Homeland Security, *U.S. Department of Homeland Security Agency Financial Report Fiscal Year 2014* (Washington, DC: DHS, February 2015).

[117] Ted Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken NJ: Wiley-Interscience, 2006), 145.

[118] John Mueller and Mark Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (New York, NY: Oxford University Press, USA, 2011).

[119] Ibid., 84.

attacks on the scale of 9/11 at least once a year, or 18 Oklahoma City bombings every year.[120]

Properly understood, this formula allows homeland security to responsibly allocate funding while making America safer. In such methodology risk becomes the province of experts: those able to know, assess, and determine the how likely and how bad something might be. Risk, then, is how such expertise makes it possible to rationalize and take action, even in uncertainty.

The appeal of risk-based security is clear to the policy maker and to the security professional. It supposes a level of rationality to both uncertainty and operational response. On its surface it provides a rule for understanding and regulating security expenditures, which should properly be scalable to the level of risk for any given threat or hazard. Understanding probability distributions of given events, and being able to analyze in detail the potential consequences, even of extreme events, allows security professional to understand where their investments should focus, not simply in terms of the capability to be built, but in terms of whether a risk is better accepted, managed through response, reduced through mitigation, or dealt with through a cost effective combination of measures.

The concept of a tornado safe room provides an elegant example of this kind of analysis; demonstrating multiple risk management measures at one location. The cost of designing a home to withstand a tornado is prohibitive when calculated by the square foot. What this means is that it is financially a better alternative to invest in insurance, disaster recovery, and hardening only a small portion of the home to be a tornado safe room.[121] If supported by enough knowledge, risk analysis should guide security professionals in knowing how much they have reduced risk through mitigation, and how much to invest in what kinds of incident management capabilities, from fire suppression capabilities to emergency procedures.

[120] John Mueller, and Mark Stewart. “Hardly Existential,” *Foreign Affairs* (April 2, 2010).

[121] Federal Emergency Management Agency, *Taking Shelter from the Storm: Building a Safe Room for Your Home or Small Business* (Washington, DC: FEMA, 2008).

1. Risk Informed Security

Risk's emphasis on decision-making illustrates that risk is a thing to be mastered not avoided—tamed not eliminated. Enterprise Risk Management is one method, or approach that views risk as an essential component to generating value. Organizations must take calculated risks in order to be successful. As expressed by the Committee of Sponsoring Organizations of the Treadway Commission, "risk is integral to the pursuit of value," and, "strategic-minded enterprises do not strive to eliminate risk or even to minimize it, a perspective that represents a critical change from the traditional view of risk as something to avoid."[122] Recent DHS approaches to risk have echoed this proactive sensibility.

The DHS chaired Interagency Security Committee (ISC) maintains federal guidelines for determining the level of risk and corresponding required level of security for federal facilities.[123] This risk management approach assigns a level of required security (I-IV) based on assessing the characteristics of the facility and its likelihood as a target.[124] The ISC process allows for an "intangible adjustment," an interesting acknowledgment of the concept that formal risk management may not be sufficient to account for either anxiety or possibility. The process also allows for a Level V designation, although what security measures are required with a Level V designation are left somewhat vague.[125] In short, the ISC process allows for something other than calculation—from expert opinion to hunches—to inform security designations.

In selecting a facility, the ISC process allows for the determination that a risk is unacceptable, but in the absence of a suitable alternate facility, a Federal entity can

[122] Deloitte & Touche LLP, Committee of Sponsoring Organizations of Treadway Commission, *Risk Assessment in Practice* (New York, NY: Deloitte & Touche LLP, October, 2012), 1.

[123] Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, DC: Interagency Security Committee, August, 2013).

[124] Ibid., 6.

[125] Ibid., 14. According to the ISC standard, "...criteria and decision-making authority for identifying Level V facilities are within the purview of the individual agency."

choose to accept that risk. Risk acceptance is an important option in this decision-making. What it acknowledges is that a certain activity or facility might be important enough to warrant taking additional risks. It is an expression of the value of the activity.[126]

Similarly, Argonne national laboratory maintains three indices that allow for DHS Protective Security Advisors to assess, “high-risk critical infrastructure assets.”[127] Protective Security Advisors conduct enhanced assessments of facilities to collect and score information about that facility. The methodologies prescribed by Argonne provide a Protective Measures Index (PMI), a Consequence Measurement Index (CMI), and a Resilience Measurement Index (RMI. In keeping with the DHS approach to understanding risk, these indices consider risk as a combination of threat, vulnerability and consequence, and the indices as a combined means of measuring and assessing these three factors in relationship to a particular site or facility. The methodology is designed to provide an all hazards approach to measured risk. The PMI methodology, for instance measures five categories of protective activity, each with second and third level subcomponents. Physical security measures include a sub component of fences, gates, and closed circuit televisions that in turn have multiple characteristics which the PMI methodology assesses and scores.[128] The utility of these indices is somewhat limited. They can provide an assessment of how individual parts of a facility perform and are resourced, but it does not necessarily highlight the overall criticality of individual components, or describe the way that they interact. Combined, however the value of this detailed triumvirate of method (PMI, CMI, and RMI) is to provide risk awareness at the facility level. Collecting information to support these indices then allows facility owners and operators to compare the performance of the facility in different scenarios using a web-based tool. In this sense, the purpose of detailed facility knowledge is a springboard

[126] Ibid., 18.

[127] F. D. Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability* (Oak Ridge, TN: Argonne National Laboratory July 2013).

[128] Ibid., 11.

to understanding and modeling system performance in different scenarios. This should guide decision-making, and provide security professionals with access to the assessment information a detailed sense of facility level risks nationwide.

2. A Noble Mirage

Thus, far, risk sounds appealing, even inspiring. It is a liberating concept, as well as a means for homeland security to advance and exert a structured control over dangers while ensuring efficient operations and spending. It is the source of sufficient confidence to guide decisions and permit value to exist as a function of risk and return. What, then, is disaster? What could 9/11, or tornados in Joplin Missouri mean in the language of risk? Is catastrophe just chance we could not tame? Are ambiguous threats the leftover uncertainty security organizations were unable to render into risk? If security were purely a matter of risk, then such losses might be considered acceptable in the grand scheme—the necessary endurance of uncertainty.

Risk has always been fickle.

Early on in the story of risk, the transition out of pure causality presented a problem of fatalism. Again, Hacking observes, "if it were a law that each year so many people must kill themselves in a given region, then apparently the population is not free to refrain from suicide."[129] Of a sudden, probability presented the same challenges to human agency that causality had before the invention of risk. This serves as a reminder that risk contains a constant element of uncertainty. It is over this question of uncertainty that the idea of risk-based security begins to suffer.

a. Risk-Based Screening

Recognizing a downward trend in security budgets and upward trends in mission requirements, the TSA has sought ways to maximize value for the public derived from transportation security. This problem gave birth to the concept of risk-based screening

[129] Ian Hacking, *The Taming of Chance*, x.

procedures.[130] There is a security proposition in this approach: If Umar Farouk Abdulmutallab, the infamous "underwear bomber" of December, 2009 would have been detected by a pat down, but the solution of patting down every traveller is unacceptable, then we need a smarter method for deciding who to pat down.

The TSA approach is built on the recognition that DHS is not as organizationally agile as an adversary. Terrorists can rapidly adapt to security procedures that take months and years to put in place. And they can keep adapting. Keeping up is, perhaps, not possible for governments. And so TSA's approach proposes that we stop chasing "devices" when faced with an infinitely adaptable enemy. Rather, TSA aggregates people (passengers) based on risk indicators. If they cannot screen everyone for the infinitely small possibility that someone is a terrorist, then they can address a challenging security tradeoff.

Innovations that allow smaller and smaller amounts of explosive to disable a plane means that TSA must better focus technology on a smaller population, and be able to absorb a lower detection rate.

TSA identifies higher risk groups of passengers, and subjects that higher risk group to a higher level of scrutiny. This allows TSA to focus resources on highest risk populations, and realize the greatest value per inspection dollar. The benefit is easy to argue. This would improve the efficiency of process, and focus resources on risks.

But here is where we might object.

If pre-check programs and other screening factors put travellers into low-risk pools, then the infinitely adaptable enemy will simply seek to place bad actors in low risk pools, while TSA excessively screens passengers who pose higher risk, but potentially no threat. This possibility was realized recently, as two men were arrested in a gun

[130] Kenneth C. Fletcher, "Aviation Security: A Case For Risk-Based Passenger Screening" (master's thesis, Naval Postgraduate School, 2011).

smuggling operation that relied on one of them having a security clearance, and airport access.[131] Adaptable adversaries can even adapt to risk-based screening.

As a matter of public accountability, the risk-based screening approach is a mixture of good and bad. The risk-based screening approach at TSA is designed to maximize the airline industry performance measures and passenger convenience. Unfortunately, while trying to maximize this value, it is simply attempting to minimize inconvenience. The essential problem with this approach is that it reduces security to a question of how much we can afford to degrade system performance. It is important to demonstrate the security return on dollars spent, however, we must also make the case that measuring the performance of security measures include measuring more than how much they degrade system performance. Security needs to be a measurable value, and acceptable risk needs to become a more common concept. How can TSA demonstrate value in the absence of thwarted attacks? If enterprise risk is meant to show value as a function of risk and return, then what is the value?

b. Risk-Based Limits

Risk-based security diminishes as an idea in the face of high uncertainty and catastrophe. Homeland security is necessarily preoccupied with the unlikely. As Lee Clarke examined in *Worst Cases*, it is the statistically unlikely plane crash, the improbable catastrophe, and the previously unimagined terror that moves security organizations to action. And plane crashes, argues Clarke, must be investigated not because of their probability, but despite it.[132] This places homeland security in a challenging position. Homeland security risk, it seems, is often not fully risk at all. It remains as uncertainty and danger. And this is at the heart of the challenge to risk-based security practices. If homeland security is predominantly in the business of the unlikely,

[131] Ashley Halsey III, "TSA tightens security amid discovery of airport gun smugglers," *Washington Post*, July 14th, 2015. Accessed August 4, 2015. http://www.washingtonpost.com/local/trafficandcommuting/tsa-tightens-security-amid-discovery-of-airport-gun-smugglers/2015/07/14/07a71cda-2a58-11e5-bd33-395c05608059_story.html

[132] Clarke, *Worst Cases*, 20.

then it is problematic to think of ordering its capabilities against likely outcomes—even a suite of likely outcomes. There is a fondness for describing events that violate predictability as “rare” events. In some case, admitting to the increasing, perhaps disproportionate, impact of these outliers, we refer to them as “forcing events” or “low probability, high consequence” events.[133] Active shooters and asteroid strikes. Terrorism and tsunamis. Such outliers are not made more acceptable by their rarity.

This seems problem enough. However, understanding the likelihood and impact of risks is also increasingly difficult. The fundamental dimensions of risk as described by DHS doctrine—likelihood and consequence—are uniquely unavailable in the case of some of the most important homeland security risks. Terrorism risk is especially uncertain, and its potential losses highly concentrated. Pandemics and cyber threats may be highly volatile and decentralized. Environmental disaster may present invisible dimensions and long latency. In other cases, even the scope of the impact defies calculation.

Curiously, the more we know about possible futures often means the less we know what to do. 100 years ago there was, literally, nothing to be done about asteroids. Today, we might be able to break them up in outer space, see them coming a few days away and order evacuations etc. But asteroids must line up alongside hurricanes and drought and climate change and terrorist attacks and mutating germs. They must compete for our attention and resources Sometimes, the more we know, the less we know what to choose. We can be equally paralyzed by knowledge and uncertainty.

Modern risks present previously unknown challenges to taming chance. Tools designed for managing calculable dangers may be unsuitable for managing highly uncertain, catastrophic, volatile or diverse threats. In homeland security, risk, it seems, is becoming unbound.

[133] Francis Fukuyama, *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2008), 1.

B. UNBOUNDED RISKS

The cockpit door locking system and entry keypad on the Airbus a320 (involved in the Germanwings 9525 crash) aircraft has built in safety features for emergencies:

> In case of emergency (suspected flight crew incapacitation, for example), a three-digit code followed by ‘‘#’’ can be dialled on the digital keypad. The acoustic signal then sounds continuously in the cockpit for 15 seconds and the green LED on the keypad starts to flash. If the flight crew does not respond during these 15 seconds, the door unlocks for 5 seconds. The green LED lights up continuously to indicate the door has been unlocked and the acoustic signal stops. The door only needs to be pushed in order to open it. After these five seconds have elapsed, the door locks again. If the flight crew toggles the switch during those 15 seconds, the acoustic signal stops and the system reacts according to the command (UNLOCK/LOCK).[134]

In short, the system is designed to allow flight crew outside the cockpit to enter if the door is locked, unless the flight crew in the cockpit prevents them. U.S. regulation and industry rules require two crewmembers in the cockpit at all times, but at the time, European regulations did not.[135] Shortly after the Germanwings accident, the European Aviation Safety Agency issued emergency guidance recommending two crew members be in the cockpit at all times.[136] The review of such safety procedures in hindsight belies a darker concern: procedures must consider more fully how to protect *against* the pilot. This is a staggering thing to consider. The professional most directly responsible for the safety of the plane must be thought of as a liability.

Of course the idea of a traitor is nothing new. Nor are negligence, operator error, fatigue or forgetfulness.[137] Nevertheless, the idea of protecting an airplane from its pilot

[134] Ibid., 17. The French government provided an English translation of the preliminary report as a courtesy, however the original French language version cited contains the official report language.

[135] Flight crewmembers at controls, 14 C.F.R §121.543 (2013), and Jon Ostrower, “United Shifts Two-Crew Cockpit Policy on Certain Boeing Jets,” *Wall Street Journal* (March 27, 2015), sec. Business.

[136] EASA Safety Information Bulletin SIB No.: 2015-04 Issued: 27 March 2015. Transport Canada, along with New Zealand Civil Aviation Authority and Australian airlines followed suit in 2015.

[137] Flight Crew Member Duties, FAR 121.542 / FAR 135.100. This regulation is known as the “sterile cockpit rule,” outlining requirements flight crew to refrain from nonessential activity during flight.

demonstrates a problem. Who guards the guards? Delivering the keynote address at the 2015 RSA conference, Amit Yoran acknowledged that one of the central errors in information system security is the amount of trust given to the trusted. What he is observing is the increased risk that occurs with localizing power, access, and capability with individuals without providing mechanisms for controlling them.[138] His observation that that the current approach to such threats places security in the "dark ages" illustrates the challenge of worst-case thinking. Fortifications are medieval. In unbounded risks insecurity is normative. In a world of worst cases, this is not a peripheral concern. For the regulator, the policy maker, the designer of procedures, or the security specialist, the importance of worst-case scenarios is a central occupation.

Fortress thinking still permeates the American approach to security. After 9/11, security measures in the cockpit of airplanes were designed like medieval castles—to provide the decision and tactical advantage to the defender within the cockpit.[139] The crash of Germanwings 9525 offers a troubling critique of this model, tied to the changing nature of modern risk. In the worst-case world of Germanwings 9525 the defender *was* the threat. The passengers on Germanwings 9525, and indeed every flight, are uniquely separated from the means controlling the risks they face. They inherit a risk that originated elsewhere, including the mental state of the pilot, and the failure of existing procedures to recognize his state, and the comparatively normal dangers posed by an airplane crash. Unbounded risk is a way of describing such risk.

1. The Insufficient Fortress

Fortifications must adapt with the threats they face. Writing in the late 19th century, French architect and engineer Eugène-Emmanuel Viollet-le-Duc considered the problem and challenge of securing a single geographic location over generations. In his book *Annals of a Fortress*, he imagines a fictional hilltop town in France, and evaluates

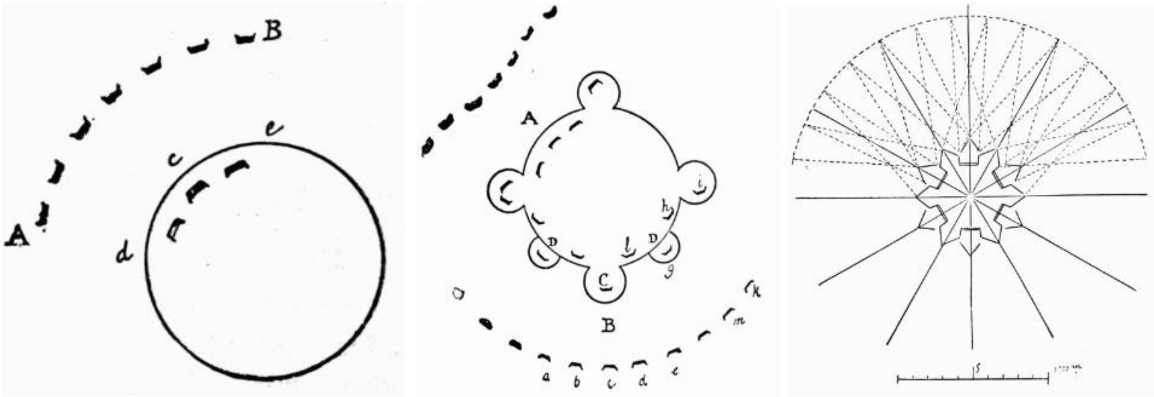
[138] Amit Yoran, "Escaping Security's Dark Ages" (speech, USA 2015 RSA Conference, April 21, 2015).

[139] Even industry standards in the U.S, which require two people in the cockpit at all times, do not fully contemplate the idea of an aggressor (or indeed two aggressors) in the cockpit.

twenty-two centuries of evolving defenses necessary to secure it from attack.[140] As a primer in the principles of fortification, the book provides a useful chart to the necessary adaptations that follow advances in technology, and evolutions in threat. As societies rise out of primitive times and into siege weapons and eventually artillery, the fortress evolves from a druidic settlement to simple Roman Oppidum, and then toward increasingly sophisticated and complicated battlements designed to counter siege weaponry. Scattered watchmen outside the campfires give way to guards and gates.

Concluding the book, Viollet-le-Duc examines the essentials of fortress thinking. In its simplest abstract form, a circular enclosure presents a defensive problem. The defender of a fortress is at a disadvantage. Facing an attacker with projectile arms, "the defenders will be able to oppose only an inferior number of engines to the convergent fire."[141] *Annals of a Fortress* illustrates this point by demonstrating the necessary changes from simple defenses to complicated defenses.

Figure 2. From Eugène-Emmanuel Viollet-le-Duc, *Annals of a Fortress*.



With this series of figures, Viollet-Le-Duc demonstrates the way that the application of the principles of fortification leads to progressively more complicated defenses. Translated by Benjamin Bucknall, *Annals of a Fortress* (Boston, J. R. Osgood and Company, 1876), Figures 77, 78, and 79.

[140] Eugène-Emmanuel Viollet-le-Duc, *Annals of a Fortress*, translated by Benjamin Bucknall. (Boston, MA: J. R. Osgood and Company, 1876).

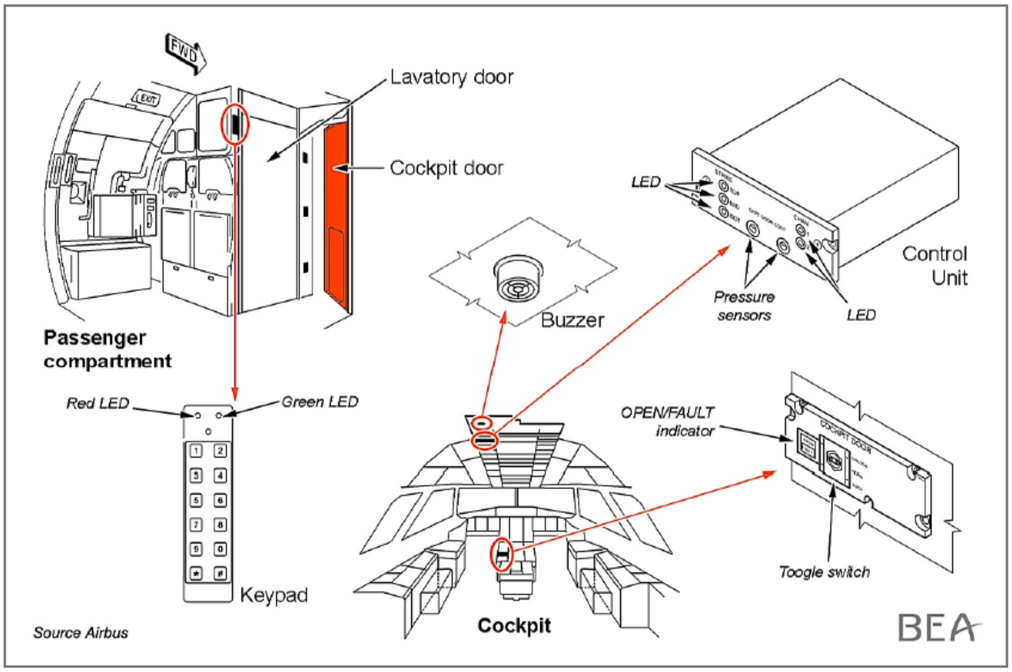
[141] Ibid., 359.

"This principle," says Le Duc, "regulates and will always regulate attack and defence; distances alone modify its applications."[142] In other words, the variation of defensive measures increases the safe distance of the attacker. Increases in the effective distance of projectile arms, from siege warfare through the development in artillery necessitate corresponding evolutions in defenses. The fortress evolves from simple to complicated as technology and tactics alter the paradigm of defense.

Completing his examination at the close of the 19th century, Le Duc concludes that the struggle between attacker and defender—and the necessity of fortifying a location against evolving threats—will result in the betterment of nations. Such conflict cultivates innovation, and the evolution of society will, he reckons, progress toward ever more complicated measures and means of defense and security. Since the publication of *Annals of a Fortress*, however, the nature of threats and risks has changed, and may require something more than complicated defenses. The 20th and 21st century have witnessed evolutions beyond technical advancements in the range and lethality of weaponry, and generated risks where the central concern is no longer robustness or complication of defenses, but the unforeseen possibilities that come with complex systems, concentrated vulnerabilities, and uncertain risks. The principle of attacker and defender is potentially eroded by complex risks, exhibited in the concentrated, unaccountable example of Germanwings, where the pilot was able to create astonishing tragedy, not despite complicated fortification, but because of it.

[142] Ibid., 360.

Figure 3. From BEA, Preliminary Report on the Germanwings Flight 9525 Crash.



Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile (BEA), *Rapport préliminaire Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l'Airbus A320-211 immatriculé D-AIPX exploité par Germanwings* (Paris, FR: BEA, May, 2015), Figure 3. Cockpit Door Locking System.

One lesson of the Germanwings tragedy is that even complicated fortification is newly insufficient. A security arrangement that made the cockpit more robust also allowed the unthinkable. The character of modern dangers exhibits the incompleteness of complication and robustness as a defensive response. Complexity, unseen connections, and ambiguous dangers, are increasing in their security prominence. Adaptive defenses seem to require a new set of tools beyond the challenge of reconfiguring our fortresses.

In 2015, the Secret Service Protective Mission Panel released the executive summary to a report.[143] The panel was commissioned to address recent security lapses (including a particularly successful fence jumper) and provide some insight into hiring a

[143] Mark Filip, Joseph Hagin, Danielle Gray, Thomas Perrelli, *Executive Summary to Report to the Secretary of Homeland Security* (Washington, DC: United States Secret Service Protective Mission Panel, December 15, 2014).

new agency director. As an opportunity to review what might be the most complex physical security problem in the modern world (maintaining perfect security at a presidential residence that welcomes well over a million visitors a year), the report offered only a few interesting observations. The recommendations summarized fall into three unremarkable categories:

- Training and Personnel
- Technology, Perimeter Security, and Operations
- Leadership[144]

Such recommendations could probably have been discerned without a formal panel report. The recommendations for leadership prescribe a mission-based budget redesign, and suggest that the next director come from outside the agency. What follows sounds suspiciously like a call to tighten procedures. But procedures may have been the problem on September 19th, 2014. Perhaps what allowed Gonzalez to reach the White House was not a failure to implement procedure, but responders adhering too rigidly to procedure, and being uncertain in the face of an event that violated procedure. Perhaps they were surprised. The reaction directly after the event (and in the Panel report) from physical security specialists was in part to widen the perimeter. The flaw in this thinking is immediately visible. The White House cannot be infinitely hardened. Deployed against a specific threat defensible space and other hardening measures reduce risk, and make theoretical sense. Deployed as a general tactic and security philosophy, they approach absurdity as threats evolve. In reviewing the incident, the Secret Service Protective Mission Panel acknowledged the limitations of a singular focus, concluding that, “For sure, the fence must be taller…But the problems exposed by recent events go deeper than a new fence can fix.”[145] There is Aegean stables efficiency to wholly rethinking missions. But there is a change in risk that remains unacknowledged in a report summary that calls for new ideas, but largely recommends a new boss, better training, and a higher fence.

[144] Ibid., 7.

[145] Ibid., 3.

The now viral video of a Buckingham Palace royal guard subtly, subversively dancing within the rigid regularity of his age-old ornamental security beat may offer some insights for refining fortresses.[146] While the guard was removed from his post for the breach in decorum, his performance illustrated a level of comfort and improvisational skill that may in fact be required by risks that do not conform to the rules of fortress thinking.

2. Risk Society

It was the same year as the Chernobyl disaster that Ulrich Beck published the German manuscript of his *Risk Society*.[147] In it, Beck considered the societal and governmental implications of living with persistent and omnipresent risks. Two decades later, Beck considered a U.S. congressional committee tasked with investigating how the U.S. might communicate to civilizations 10,000 years in the future the hazards associated with our nuclear waste, wondering, "what concepts can we form, and what symbols can we invent to convey a message to people living 10,000 years from now?"[148] Considering the dimensions of such a problem Beck offers a summation of the problem of modern risks:

> What is remarkable about this commission is not only its research question, that is, how to communicate across 10,000 years, but the scientific precision with which it answered it: it is not possible…Past decisions about nuclear energy and present decisions about the use of gene technology, human genetics, nanotechnology, etc., are unleashing unpredictable, uncontrollable and ultimately incommunicable consequences that might ultimately endanger all life on earth.[149]

[146] Alastair Macaulay, "At Buckingham Palace, a Dancing Guard Throws Decorum to the Wind," The New York Times, September 16, 2014.

[147] See Ulrich Beck, *Risikogesellschaft: Auf dem Weg in eine andere Moderne* [risk society: towards a new modernity] (Frankfurt, DE: Suhrkamp Verlag, 1986). For the first English edition see also Ulrich Beck, *Risk Society.*

[148] Ulrich Beck, "The Terrorist Threat World Risk Society Revisited," *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[149] Ibid.

Modern risk as defined by Ulrich Beck was, "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself."[150] Here risk is not a general method for making sense of the world, but a necessary construction around the dangers which human society introduces as it advances. And Beck was struck by the profound social implications of society dealing with risks it has created. One of his most striking observations notes the way that in modern risks, the cause and effect of risks become separated. The Bhopal chemical disaster, argues Beck, demonstrates the way that a globalized economy can transition the production of dangerous chemicals to third world countries, where the catastrophic impact of a factory accident then poisons an unwitting population living near the plant.[151] Managing such scattered risks becomes problematic.

a. Risk Society and Unbounded Risk

Risk Society was revolutionary in its scope, but it also reflected a growing trend in observations of the time concerning the nature of extreme risks posed by increasingly complicated technological hazards.[152] The heightened possibilities associated with technological accidents put in high relief the idea that mankind was able to create dangers more powerful and complex than the measures for control he might be able to design. Technological risk had transitioned in some way from mere complication to complexity, which implied that aspects of risk were invisible. The safety procedures surrounding modern technology—from nuclear power to chemical production—presented a challenge to risk because they made it difficult to assess the probability and consequences of an incident. But it was not simply a Frankenstein terror, or fear of a machine run amok. Rather Beck was interested in the idea of what a society that was no longer feudal or industrial would do with the idea of risk. How might risk transform social arrangements or governmental structures? Risk presented itself in this thesis as something more than a

[150] Ulrich Beck, *Risk Society,* 21.

[151] Ibid.

[152] Patrick Lagadec, *La civilisation du risque: catastrophes technologiques et responsabilité sociale* [the civilization of risk: technological disasters and social responsibility] (Paris, FR: Seuil, 1981), and *Major Technological Risk: An Assessment of Industrial Disasters* (Oxford, UK: Elsevier Science Limited, 1982).

problem to be capitalized on, instead a new social phenomenon that governments, organizations and individuals must organize their lives by.

Beck contends that, "calculating risks is part of the master narrative of first modernity."[153] But risk society represents what Beck refers to as "second modernity," a period defined by the societal self-awareness of coping with the risks it has created. And here Beck considers the ways in which modern risks appear to defy the established methods of calculation and control. Observing that risks are increasingly de-localized, incalculable, and non-compensable, Beck viewed them as "de-bounded" along multiple dimensions: spatial, temporal, and social.[154]

Spatially, risks do not conform to political boundaries, or the doctrinal and operational distinctions between professional disciplines and infrastructures. The Ebola virus, once consigned to burn out in remote villages, now moves at the speed of transportation, evolving rapidly into a problem of logistics, border security, intelligence and interdisciplinary coordination.[155] Climate change, along with toxic pollution and even the transport of hazardous materials illustrate the ease with which risks move, and shift across spatial boundaries.[156] Temporally, the long-term impacts of nuclear and biological attacks and accidents produce long-term effects that further complicate attempts to understand their impact. The social dimension of risks serves both to make it difficult to locate the precise source of risks, and easy for risks to be amplified by complex social dimensions.

American sociologist Kai Erikson considers the ways in which chemical and radiological disasters, "violate all the rules of the plot," of risk:

[153] Ulrich Beck, "The Terrorist Threat World Risk Society Revisited," *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[154] Ibid.

[155] Interview Conducted by Rafaela von Bredow and Veronika Hackenbroch, "Interview with Peter Piot Discoverer of the Ebola Virus," Spiegel Online (September 26, 2014).

[156] *National Climate Assessment*, Accessed July 1, 2015. http://nca2014.globalchange.gov/node/1961.

> Some of them have clearly defined beginnings, such as the explosion that signaled the emergency at Chernobyl or the sudden moment of realization that opened the drama of Bhopal; others begin long years before anyone senses that something is wrong...But they never end. Invisible contaminants remain part of the surrounding, absorbed into the grain of the landscape, the tissues of the body, and, worst of all, the genetic material of the survivors. An all clear is never sounded. The book of accounts is never closed.[157]

These curious modern risks appear to violate the very dimensions which homeland security organizations are positioned to measure. The Argonne methodologies of PMI, CMI and RMI depend on an ability to measure threat, vulnerability and consequence with sufficient accuracy to guide decisions. But in Beck's risk society, threats are highly uncertain, consequences are incalculable, and vulnerabilities are occluded. As Kai Erikson observes, the consequence of risks may never be counted as complete, their onset may be of indeterminate latency. In a risk society, calculations will often be incomplete.

The phenomena of such risk is exemplified by chemical and radiological events, but it is not restricted to them. As recently as September of 2014, FEMA and the State of Louisiana still retained $812 million in unexpended hazard mitigation grant program funds, nearly a decade after Hurricane Katrina.[158] The impact of modern disasters extends beyond the initial assessments, calculations, and the operational conduct of emergency response. From chemical disaster to Katrina and 9/11, the book of accounts remains open.

[157] Kai T. Erikson, *A New Species of Trouble: The Human Experience of Modern Disasters* (New York: NY: W.W. Norton & Company, 1995), 148.

[158] Department of Homeland Security, Office of the Inspector General, *FEMA and the State of Louisiana Need to Accelerate the Funding of $812 Million in Hazard Mitigation Grant Program Funds and Develop a Plan to Close Approved Projects* (Washington, DC: DHS, September, 2014).

b. Risk Society and Double Government

In the attacks of 9/11 Ulrich Beck saw the implication that, “a state can neoliberalize itself to death.”[159] The thesis of *Risk Society* meant that the state would increasingly need to assert itself. Government institutions would supersede private or economic concerns in order to provide security. With the creation of DHS, new agencies like the TSA, and other reactions to 9/11, this seems demonstrably true. Government has reordered itself around an assertion of domestic security. However, because government institutions like DHS are established to provide security, in a risk society, “every accident violates the basis of the unshakeable right to security which appears to be promised.”[160] That is, departments and agencies designed expressly to promise security to citizens find themselves unable to deliver on their promises in increasingly prominent ways.

Because unbounded risks create such immense challenges in the realm of calculation and response, they have the curious quality of increasing the distance between the citizen and the government entities designated to provide security. Considering the question of why security policy has not appreciably changed between two presidential administrations, Michael J. Glennon reaches a disturbing conclusion: it is not the president, nor the judiciary, nor even the congress, who exert the most sway over national security policy.[161]

The American experiment, describes Glennon, designated a three-part separation of governmental power between the “dignified” “Madisonian” institutions of Executive, Judicial and Legislative branches. Security, since the days of Harry Truman and the national security act of 1947, has become the emphatic province of the expert—the “efficient” “Trumanite” institutions of government that exist in executive branch security agencies. Invoking the 19th century observations of Walter Bagehot, Glennon concludes

[159] Ulrich Beck, “The Terrorist Threat World Risk Society Revisited,” *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[160] Ulrich Beck, “Living in the World Risk Society,” *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

[161] Michael Glennon, *National Security and Double Government* (New York, NY: Oxford University Press, 2014).

that America is under the grip of a "double government." While the "dignified" institutions of the "Madisonian" scheme continue to function, their purpose is largely symbolic. Meanwhile, the actual decisions and calculations about risks are managed by the network of government experts in the "Trumanite" government. Americans are being governed twice. And the means of oversight for these institutions—ultimately culminating in the right and duty of American citizens to vote—is undermined by the inability to directly access this second veil of government. Representatives in the legislature are, according to Glennon, less and less equipped to intrude upon the "Trumanite" network.

One challenge to Glennon's concern is the apparent necessity of "Trumanite" efficiency in the face of unbounded risks. Arguably, unbounded risk is complicated and uncertain in such a dramatic sense, that it has become solely the province of experts, and far beyond the legislative skill set of Congress, or the well-intentioned decision making of the President. Cass Sunstein has recently expounded on this very idea, arguing that the executive branch has by necessity grown to be the "most knowledgeable branch."[162]

Increasingly uncertain risks—from technological complexity to decentralized non-state threats and violent extremism—particularly challenge the way that government response to them. "Unlike specific dangers," says Mikkel Rasmussen, "which can be countered by specific means, threats are elusive, compelling risks that must be managed."[163] The impact of such risk elusiveness is, according to Beck, a profound social change in what risk means. Citizens and elected officials alike are so unable to be fully expert in risks—from technological systems and biologically engineered germs to sectarian rivalries and cyber vulnerabilities—that they relinquish to the experts. The more startling conclusion, as Beck points out, is that even experts are unable to perfectly predict terrorist threats or technological disaster, and, "when there is no one to give the

[162] Cass Sunstein, "The Most Knowledgeable Branch," *SSRN Scholarly Paper* (Rochester, NY: Social Science Research Network, July 14, 2015).

[163] Mikkel Vedby Rasmussen, "'It Sounds Like a Riddle': Security Studies, the War on Terror and Risk," *Millennium - Journal of International Studies* 33, no. 2 (March 1, 2004): 381–95.

authoritative answers then society begins to work in new ways, it ceases to be modern and becomes reflexive about its own modernity."[164]

Unbounded risks create a separation between the instruments of security and those secured by it. Citizens in a risk society are separated from the government that provides security. Information that must be classified is remanded to the specialists who have been investigated and vetted. It is not so much hidden from the citizen, as it is hidden from the adversary who would misuse it, but in the process, the citizen is separated from the specialized world of security management trained and equipped to handle such vagaries. In the realm of national security, as the equipment necessary to combat risks becomes increasingly arcane, the arrangements increasingly byzantine, and the risks more abstruse and uncertain, so too does the distance between the governed and the government tasked with providing security widen.

In Beck's view unbounded risk undermines the concept of liberal government. Says Beck:

> It is easy to misconstrue the theory of world risk society as Neo-Spenglerism, a new theory about the decline of the western world, or as an expression of typically German Angst. Instead I want to emphasize that world risk society does not arise from the fact that everyday life has generally become more dangerous. It is not a matter of the increase, but rather of the de-bounding of uncontrollable risks.[165]

Beck is not predicting the decline of the West, but rather concludes that unbounded risk that did not respect political boundaries required governance that did not respect political boundaries. The globalization of risks demands a corresponding globalization of governance. The problem of climate change is not geographically constrained, its causes and effects not political. Likewise, the spread of Ebola in 2014 illustrated the permeability of doctrinal and organizational distinctions. Security agencies have responded largely along the lines that Beck argues may be necessary. Despite its resurgence, Beck saw here the end of the idea of the national state, as government

[164] Ibid.

[165] Ibid.

institutions become, “more powerful, and supranational institutions like NATO [become] less powerful.”[166]

Beck imagined a “cosmopolitan” form of government—one that corresponded not to national state boundaries, or parochial interests, but to the dimensions or risk and the complexities of an increasingly connected society. The nationalization of the NIMS and the ICS are indicators of a similar impulse to create a form of governance for risk that does not correspond to jurisdiction. The creation of national systems and increasingly trans-political security measures and approaches indicate a trend toward adjusting security governance measures to match the scale of risks.

The impulse is incomplete. NIMS, ICS, and other increasingly globalized, or systematized security management approaches are not multilateralism or cosmopolitanism, but merely a competing form of unilateralism. Such systems fail to address other essential characteristics of unbounded risks—characteristics that demand variability, and adaptability.

Ultimately, a re-invigorated sense of federalism—a jumpstarting of the “dignified” “Madisonian” institutions—may be the only answer to enduring uncertainty. It may also provide the kind of cosmopolitanism Beck aspired to, redistributing the centralizations that have been carried along by the resurgence of the state in the wake of 9/11. Decades before Beck, John Maynard Keynes considered the importance of uncertainty which cannot be eliminated, despite probabilism and analysis:

> By ‘uncertain knowledge’, let me explain, I do not mean merely to distinguish what is known from what is merely probable. The sense in which I am using the term is that in which the price of copper and the rate of interest twenty years hence, all the obsolescence of a new invention are uncertain. About these matters there is no scientific basis on which to form any calculable probability whatever. We simply do not know.[167]

[166] Ulrich Beck, “The Terrorist Threat World Risk Society Revisited,” *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

[167] John Maynard Keynes, “The General Theory of Employment,” *The Quarterly Journal of Economics*, Vol. 51, No. 2 (February, 1937), pp. 209-223, Published by: Oxford University Press.

Homeland security theory must consider more directly this margin of enduring uncertainty. Current approaches tend to view it as residual—best managed through accelerated and rapid versions of standard risk management and crisis response tools. Other influential theories may provide a more refined engagement with uncertainty. "Crises," says Patrick Lagadec, "seem to be in total opposition to the very foundations of modern social science."[168] This is because the persistence of complexity and the endurance of uncertainty continue to undermine the evolving measures to centralize means of controlling interconnected and mercurial risks.

3. Worst Cases

Contemplating the possible destruction of the earth, Cambridge physicist Adrian Kent notes drily that in addition to the loss of all life on the planet, "there is the opportunity costs arising from the absence of future generations."[169] This is a cost beyond accounting. Kent considers two opposing views of such world ending possibilities:

> Proposed catastrophe mechanisms generally rely on speculation about hypothetical phenomena for which there is no evidence, but which at first sight do not contradict the known laws of physics. Sometimes, such pessimistic hypotheses can be countered by arguments which show that the existence of the catastrophe mechanism is highly improbable, either because closer analysis shows that the proposed mechanism does in fact contradict well established physical principles, or because its existence would imply effects which we should almost certainly have observed but have not.[170]

The question Kent wrestles with is how to reconcile the possible with the probable. On the one hand, there are hypotheticals, on the other hand the challenge of proving, disproving and dealing with them. Kent laments that little has been done to resolve the conflict between these two views, mathematically or in terms of policy.

[168] Patrick Lagadec, "Risks and Crises in Terra Incognita," *Paris Tech Review* (October 10, 2010).

[169] Adrian Kent, "A Critical Look at Risk Assessments for Global Catastrophes," *Risk Analysis* 24, no. 1 (2004): 157–68.

[170] Ibid.

One such scenario that Kent considers is the possibility of a particle accelerator disaster. In 1999, scientists at the Relativistic Heavy Ion Collider (RHIC) commissioned by Brookhaven National Laboratory responded to concerns that heavy ion collisions could result in the end of the world.[171] Sir Martin Rees, the United Kingdom's astronomer Royal, has further explained that the RHIC could produce a, "shower of quarks" leading to a hypothetical "strangelet disaster" that could reduce the earth into, "an inert, hyperdense sphere about one hundred meters across."[172] Rees and other scientists have concluded that the possibility of a strangelet disaster is remote, but calculating this remoteness presents analytic challenges. Adrian Kent, in acknowledging that the possibility of a strangelet disaster is, within current theoretical models, "precisely zero," admits that, "When the destruction of the Earth is in question, though, it would be preferable not to have to rely on theoretical expectations alone."[173] Put simply, the outcome of a strangelet disaster is so potentially bad, even infinitesimal improbability may not be sufficient comfort.

Considering this scenario of earth's destruction, Richard Posner concludes that while such dangers appear lower, they are ultimately incalculable.[174] Incalculable dangers may be *easier* to ignore, but that does not mean that they are *best* ignored.

Neglecting such possibilities in favor of probabilities can be dangerous. In *Worst Cases*, Lee Clark argues that, "probabilistic thinking is not the only way to be reasonable."[175] Worst cases, argues Clarke, may be unlikely, but they are not aberrant. They are rare, but normal. And worst cases matter especially for security agencies and organizations. This presents immense challenges. While the temptation in confronting worst cases is to build organization of such robustness that they permit a form of

[171] Sameer Shah, "Perception of Risk: Disaster Scenarios at Brookhaven" (Paper, Massachusetts Institute of Technology, 2003).

[172] Richard Posner, *Catastrophe: Risk and Response* (Oxford University Press, 2004), 30.

[173] Adrian Kent, "A critical look at risk assessments for global catastrophes," *Risk Analysis* 24, no. 1 (2004): 157-168.

[174] Posner, *Catastrophe : Risk and Response*, 251.

[175] Clarke, *Worst Cases*, 44.

organization hubris, Lee Clarke warns that the lesson or worst cases is almost the opposite. Worst cases should make us humble[176]

4. The Fourth Dimension: Rationality

The first preseason outlook produced by National Oceanic and Atmospheric Administration for the 2012 Atlantic hurricane season predicted 9–15 Named Storms, 4–8 Hurricanes, and 1–3 Major Hurricanes.[177] The season actually produced 19 tropical cyclones. One of them was Hurricane Sandy. Sandy made landfall on October 29, 2012 as a post-tropical cyclone, and it impacted densely populated and complicated jurisdictional, infrastructural, and residential communities in New York and New Jersey.[178]

Because of the complex of storm damages, jurisdictional arrangements, and multi-state impacts of the storm, FEMA faced corresponding challenges in organizational arrangement. FEMA doctrine allows for three basic operational paradigms: functional organization, geographic organization, and a hybrid approach to each. For Sandy, FEMA opted for a hybrid approach, but applied it inconsistently and faced enormous challenges in allocating and maintaining visibility for resources across geographic and functional branches and divisions.[179]

FEMA faced an emergent property that is increasingly common to catastrophe and threat: hypercomplexity. Unconventional dangers degrade traditional, "crisis planning and management, and [make] them instantly obsolete."[180]

[176] Ibid.

[177] National Oceanic and Atmospheric Administration, *NOAA 2012 Atlantic Hurricane Season Outlook*, issued May 24, 2012.

[178] Stacy Stewart, *National Hurricane Center Annual Summary: 2012 Atlantic Hurricane Season* (Washington, DC: National Oceanic and Atmospheric Administration, January 23, 2014).

[179] FEMA, *Hurricane Sandy FEMA After Action Report* (Washington, DC: FEMA, July 1, 2013).

[180] Erwan Lagadec, "Unconventional Crises, Unconventional Responses: Reforming Leadership in the Age of Catastrophic Crises and Hypercomplexity," *Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies* (Baltimore, MD: Johns Hopkins University, 2007).

Hypercomplexity makes it difficult to establish a rational understanding of threat and catastrophe. It is difficult to develop and frame operational objectives when the problem itself is variable, and more complex than our means of understanding it.

C. CASE STUDY: CRUDE OIL UNBOUND

> *Each of us is all the sums he has not counted...the seed of our destruction will blossom in the desert, the alexin of our cure grows by a mountain rock*
>
> —Thomas Wolfe[181]

Early on the morning of July 6th, 2013, crude oil from North Dakota resulted in 47 fatalities in Quebec Canada. Unbounded risk is like this, drawing invisible lines of chance that suddenly become clear in the aftermath of tragedy. Cause, effect, assessment, and response are separated, creating national and international challenges to tracing out such lines of dependency before they result in damage and death. American novelist Thomas Wolfe wrote of the, "dark miracle of chance," in which, "every moment is a window on all time."[182] Moments of catastrophe are like this, forcing events that cause homeland security to try and trace the outline of causation to its root. Unbounded risks make it difficult to do so.

The evening prior, a 4700-foot oil transport train left unattended overnight began to roll. It travelled more than seven miles, ultimately reaching a speed of 65mph when it derailed in the center of the town of Lac-Mégantic, Quebec.[183] Its derailment set off a series of fires and explosions in which, "47 people died, and about 2000 people were evacuated. Forty buildings and 53 vehicles were destroyed."[184] The accident also resulted in contamination of a nearby lake and river.

[181] Thomas Wolfe, *Look Homeward, Angel* (New York, NY: Charles Scribner's Sons, 1929; New York, NY: Simon and Schuster, 2006), 5.

[182] Ibid.

[183] Transportation Safety Board of Canada, *Railways Investigation Report R13D0054 Runaway and Main-Track Derailment of Montreal, Maine, & Atlantic Railways Freight Train MMA-002 MILE 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013* (Gatineau, QC: August, 2014).

[184] Ibid., 3.

The accident analysis section of the investigation into Lac-Mégantic begins with a reflective acknowledgement. “Understanding what happened is only the first step;” say the authors, “it is important to determine why such accidents happen. This analysis will therefore focus on the underlying factors that played a role in this accident.”[185] The scope of the Transportation Safety Board of Canada investigation report follows this approach, and it reveals the unbounding of risk along multiple dimensions. A startling array of factors contributed to the accident and defined its impact. It is difficult to pinpoint a single cause. Examined in hindsight the accident appears as an inevitable unfolding of a complex of interactions. But the workings of these constituent parts were, in many crucial ways, invisible to the individuals and groups involved in the accident.

On the evening prior to the accident, the train was discharging an unusual amount of smoke, the result of a nonstandard engine repair that left superheated oil building up in the body of the turbocharger.[186] The engineer noted this, and planned to deal with it in the morning. The train was secured for the night using a combination of air brakes, handbrakes, and independent brakes to prevent it from beginning to roll. The engineer tested the hand brakes by removing the air brakes, but neglected to remove the independent brakes. The train did not move, and the engineer, “deemed the test successful.”[187] The engine, per procedure, was left running, maintaining compression for the air brakes. Just before midnight, firefighters responded to a 911 call and extinguished a fire on the locomotive, caused by the oil buildup in the turbocharger. Following procedure, the firefighters shut the locomotive’s fuel supply and electrical breakers off. In consulting with the rail line representative dispatched to the scene (a track foreman, not a locomotive engineer), the locomotive was left off for the night, and firefighters, along with the representative left the scene after notifying the rail traffic controller of the condition of the train. However, the air brakes relied on compressed air, which the engine was no longer producing. Additionally, a fail-safe mechanism that would engage other

[185] Ibid.

[186] Ibid., 98.

[187] Ibid.

brake systems was wired incorrectly and did not engage when the firefighters pulled the breakers. As the air brakes lost compression, the remaining brakes were insufficient, and the train began to roll.[188]

This was only the proximate cause of the accident.

The train derailment occurred at a switch point that brought a main thoroughfare in the town alongside rail track turnouts and switch points. The 47 fatalities might be blamed on this aspect of municipal and industrial planning that concentrated people near technological risk. But just as easily one might blame the design of the 63 tank cars that derailed. The joint Department of Transportation (DOT) rule developed in the aftermath of this disaster prescribes retrofit and design changes to the standard DOT-117 tank cars (TC-117 in Canada).[189] Or perhaps it is the volatility of Bakken Crude itself, or the rail safety or the fire response procedures. Perhaps even more broadly, the Lac-Mégantic disaster is not separable from the forces of global economics and geopolitics that generate the demand and permit the transport of crude oil across borders and countries.

Perhaps it is all these things. The lesson appears to be the complexity and the invisibility of connections between these contributing aspects of risk.

The unnamed repairman who performed nonstandard repairs on the engine of the MMA-002 train was likely not aware of standard procedures for responding firemen, or even the worn condition of the handbrakes on that train. Nor could he have been expected to understand the way that a more volatile form of crude oil could change the risk profile for a community the oil travelled through. Even the table of contents to this report serves as a reminder of the nature of the risk society thesis, as well as the ultimate "normal accident" and an archetypical "worst case." The design of rail cars, the physical layout of rail lines, the grade and geography of the region, safety procedures, brake designs, regulations in place, rail traffic, community planning, emergency response planning, and

[188] Ibid., 99.

[189] Department of Transportation, "Rule Summary: Enhanced Tank Car Standards and Operational Controls for High-Hazard Flammable Trains," Text, April 30, 2015. http://www.dot.gov/mission/safety/rail-rule-summary.

the corporate culture of the Montreal, Maine and Atlantic Railway are all factors which influenced the accident.

As an exemplar of the risk society, the Lac-Mégantic disaster demonstrates the challenge of addressing the enormous complexity of risks that are the product of modernity. The difficulty of managing a risk that originates in North Dakota, and exhibits itself in Quebec takes on uncertain proportions. As expressed by Ulrich Beck, "thanks to the complexity of the problems and the length of chains of effect, assignment of causes and consequences is no longer possible with any degree of reliability."[190] The fuel coming from the Bakken range is potentially more volatile than other crude oil, but it has been shipped over systems—from rail lines to tankers to human procedures and emergency response plans—that remained unchanged. The trains carrying Bakken oil transect multiple jurisdictions, each with differing capabilities to respond to crude oil fires, and with uncertain and variable training budgets and private and public resources for crisis management. The citizens of Lac-Mégantic found themselves the inheritors of those risks, suffering the effects of a disparate sea of complex causes. This is not to argue that the failure of risk management in the case of Lac-Mégantic undermines the idea of risk management. The accident investigation report highlights failures of risk assessment in multiple stages and places. But the complexity of procedure, responsibility, jurisdiction, political boundaries, law, regulation, and response, all demonstrate the many ways in which risk can become unbound from the tools available to comprehensively approach it.

As a normal accident, it is interesting to note the criticality of small decisions in the disaster. The track foreman who was not aware of the interrelationships between braking systems on the train, demonstrates the normal accident notion of tight coupling and socio-technical systems. It is startling to consider the many risks within a rail system that depend so greatly on other actions within the system. There is nothing remarkable

[190] Ulrich Beck, "The Terrorist Threat World Risk Society Revisited," *Theory, Culture & Society* 19, no. 4, August 1, 2009: 39–55.

about any individual decision or mistake in the story of the accident, however the arrangement of the rail system magnified the results of those decisions.

And finally as a worst-case this accident challenges the imagination and organizational hubris that accompany such risks. By mid-2015 the total compensation fund established for the Lac-Mégantic disaster was $435 million.[191] Probabilistic thinking, says Lee Clarke, needs the augmentation of possibilistic thinking.[192] The difficulty with the interlocking network of rail safety regulation, emergency response, public governance and private industry is that it makes it very challenging for organizations to exercise such imagination. It is difficult to think of regulating to possibility. And risk management designed to thread the needle between safety and efficiency is not always well suited to the contemplation of worst cases.

In 2014, the U.S. DOT issued a series of emergency orders and safety advisories concerning crude oil coming from the Bakken oil fields in North Dakota, culminating in final rule on May 1, 2015 designed to strengthen the safety standards governing the transportation of flammable liquids over rail lines.[193] The rule is impressively comprehensive, addressing a range of issues from the design and retrofit of oil transport tankers to crude oil testing and reporting requirements and new responsibilities for oil companies to liaise with emergency management agencies and information sharing centers in potentially impacted jurisdictions.

The rule further illustrates a vital lesson in managing unbounded risk. Put simply, such risks may not be managed in isolation. The problems of unbounded risk require unprecedented intimacy between uncommon disciplines, and across political boundaries. But the inability to foresee such necessary connections until after accidents occur means

[191] CBC News, "Lac-Mégantic Families Approve $435M Compensation Package," Accessed June 10, 2015. http://www.cbc.ca/1.3106289.

[192] Clarke, *Worst Cases*, 51.

[193] Department of Transportation's Pipeline and Hazardous Materials Safety Administration, "PHMSA - Chronology." Accessed June 10, 2015. http://www.phmsa.dot.gov/hazmat/osd/chronology, and "DOT Announces Final Rule to Strengthen Safe Transportation of Flammable Liquids by Rail," Text. Department of Transportation, May 1, 2015. http://www.dot.gov/briefing-room/final-rule-on-safe-rail-transport-of-flammable-liquids.

that identifying and creating this necessary intimacy ahead of time—in planning, operations, and response—is often impossible. In approaching such risks, unknown complexities and unseen connections ought to dominate our security considerations. In responding to such accidents, skill in working with strangers and uncommon disciplines is paramount.

D. CASE STUDY: INSURANCE UNBOUND

> *An Act to provide for the payment out of money provided by Parliament or into the Consolidated Fund of sums referable to reinsurance liabilities entered into by the Secretary of State in respect of loss or damage to property resulting from or consequential upon acts of terrorism and losses consequential on such loss or damage.*
>
> —[27th May 1993][194]

> *An Act…to ensure the continued financial capacity of insurers to provide coverage for risks from terrorism. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled.*
>
> —H.R.3210 —107th Congress[195]

The insured losses resulting from the attacks of 9/11 approached $44 billion.[196] In the midst of great national tragedy, this provided a stark and sudden lesson about the potential economic instability that catastrophic terrorism can provoke. Prior to 9/11, commercial insurance generally covered terrorism losses.[197] In the wake of devastating and concentrated industry losses, insurance and reinsurance markets began excluding terrorism from their coverage, presenting a problem for builders and developers who required that insurance to secure loans. The World Trade Center Bombing and the Oklahoma City Bombing did not generate such a response. The insurance lesson of 9/11

[194] "Reinsurance (Acts of Terrorism) Act 1993," Text. Accessed March 9, 2015.

[195] "Terrorism Risk Insurance Act of 2002," Public Law 107-297 107th Congress, Text. Accessed April 10, 2015.

[196] Howard Kunreuther, and Erwann Michel-Kerjan, *TRIA after 2014: Examining Risk Sharing under Current and Alternative Designs* (Philadelphia, PA: Wharton, University of Pennsylvania, 2014).

[197] Ibid.

was new for America. In the United Kingdom (UK), the retreat of insurance companies from providing coverage for terrorism losses was an old problem by the time 9/11 occurred, with a solution well underway.

On the morning of April 24th, 1993, the Provisional Irish Republican Army (IRA) detonated a truck bomb on Bishopsgate, a central part of London's financial district. One person was killed, another 44 injured. At the time, loss estimators imagined the damage to be slightly worse than the Baltic Gate bombing, which had targeted financial infrastructure a year prior.[198] The ultimate cost of the Bishopsgate bombing was estimated between £350 and £500 million pounds, elsewhere cited as more than $1.5 billion.[199] But for the insurance industry, these costs were also signals of a deeper problem. Paying claims on such attacks nearly initiated the collapse of the world's leading insurance market, Lloyds of London.[200] As a result, insurance companies in the UK began to remove terrorism from their list of covered losses.

This meant that if future attacks occurred, the financial exposure would go uninsured, leaving the government with the decision to reimburse or not. In a sense, the tactics of the IRA were made explicit, and the impact was felt immediately. The UK responded by establishing a government backed insurance scheme, and entering what is now a complex global response to a difficult threat.

On the 27th of May, scarcely a month after Bishopsgate, it was enacted, "by the Queen's most excellent majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same…" that the UK government was in the business of insuring against terrorism.[201] The insurance industry, in cooperation with her majesty's government,

[198] Christopher Elliott and, Richard Ford, "Police Alerted to Bomb Threat on Eve of Blast; IRA Bishopsgate Bomb," *The Times*, Apr 27, 1993.

[199] Fiona Gibson. "Pool Re Must Wait for Answer on Funding," *Lloyds List*, Dec. 15, 1993; see also Federal Emergency Management Agency, *Risk Management Series: Incremental Protection for Existing Commercial Buildings from Terrorist Attack* (Washington, DC: FEMA, April, 2008), 3-4.

[200] Ibid.

[201] "Reinsurance (Acts of Terrorism) Act 1993," Text, Accessed March 9, 2015.

established Pool Re, a reinsurance firm designed to establish an insurance market for controlling terrorism risk. Facing a sustained IRA campaign against the financial sector, the insurance industry in the UK was presented with a unique challenge. The risks associated with terrorism losses were particularly hard to insure against.

The essential difficulty was twofold. Terrorism was difficult to estimate in terms of impact and probability. And secondly, losses are spatially concentrated.[202] This meant that high value, commercial, city properties were the most likely to be attacked—the only companies asking for the insurance would be most likely to need it, a problem known as "adverse selection." Commercial terrorism insurance suddenly shared the problem of high-risk coastal areas, without sufficient probabilistic data from which to derive the cost or likelihood of the impact. Insurers and reinsurers were open to substantial losses, without a reliable means of rate setting that would make insurance affordable for the consumer or viable for the insurer.

The solution in the UK was to establish a separate company, Pool Re, which would manage a government backed reinsurance program against terrorism. This made the UK government the "insurer or last resort" for terrorism.[203] Under the system created in 1993, insurance companies applied to and became members of the Pool Re scheme. The premiums collected from that insurance would go towards covering losses in the event of an attack. Costs exceeding the collected premiums would be carried by the insurance companies who bought into the Pool Re scheme up to a 110% of the total funds in the risk pool. Costs in excess of that value would, in turn, be borne by the UK government.

In contrast, the Terrorism Risk Insurance Act of 2002 (TRIA) made the offer of terrorism coverage mandatory in the U.S. The United States established the TRIA, which, similar to the UK model, shares the costs of insured terrorism losses between the

[202] Risk Management Solutions, *Quantifying U.S. Terrorism Risk,* White Paper (Newark, CA: RMS, 2014), 8.

[203] William B. Bice, "British Government Reinsurance and Acts of Terrorism: The Problems of Pool Re." *U. Pa. J. Int'l Bus. L.* 15 (1994): 441.

government and private sector, as a means of making sure that terrorism coverage is available. The TRIA was a temporary authorization passed in 2002 and extended in 2005, 2007 and most recently 2015.[204] Part of the goal of the TRIA is to encourage a viable private sector insurance/reinsurance market. Both the UK model and the U.S. model include mechanisms for sharing the risk and impact of terrorist attacks between the private and public sectors, and both face similar challenges in attempting to grow their respective programs toward a lesser burden on the taxpayer to fund the protection against the terrorism risk.

And yet in the U.S., the TRIA is very different from the UK model. As a temporary program it did not establish a permanent company, or risk pool. The TRIA created a mandatory requirement—requiring all U.S. primary insurance companies to offer insurance against terrorism.[205]

1. Reinsurance Revolution

In March of 2015, Pool Reinsurance Company Ltd. (Pool Re) announced the purchase of terrorism reinsurance on the commercial market for the first time since its inception in 1993.[206] It is difficult to speculate just what this newly minted availability of private reinsurance within the UK means. While the industry ability to model terrorism losses has improved, this does not seem to be the reason behind the sudden availability of commercial reinsurance. The insurance industry still views terrorism risks as a, “constant, evolving and potentially expanding threat for the foreseeable future.”[207] The answer may in part have to do with Edward Snowden.

[204] Terrorism Risk Insurance Act of 2002 (TRIA), Terrorism Risk Insurance Extension Act of 2005 (TRIEA), Terrorism Risk Insurance Program Reauthorization Act of 2007 (TRIPRA).

[205] Howard Kunreuther and Erwann Michel-Kerjan, *TRIA after 2014: Examining Risk Sharing under Current and Alternative Designs* (Philadelphia, PA: Wharton, University of Pennsylvania, 2014).

[206] “Pool Re Purchases £1.8 Billion in Reinsurance,” PoolRe, Accessed March 9, 2015. https://www.poolre.co.uk/pool-re-purchases-1-8-billion-in-reinsurance/.

[207] Robert P. Hartwig and Claire Wilkinson, *Terrorism Risk: A Constant Threat, Impacts for Protерty and Casualty Insurers*, Paper (New York, NY: Insurance Information Institute, March 2014), 5.

A provocative assertion went quietly unnoticed in 2014 outside of narrow risk management circles. In its published white paper report entitled, “Quantifying U.S. Terrorism Risk” the firm Risk Management Solutions included the following assessment:

> [models of terrorism risk] tend to presume a lack of Western counter-terrorism capability to control terrorist action against the U.S. homeland. This presumption may be attributable to a dearth of public information about counter-terrorism activities. Counter-terrorism officials are duty-bound to “serve in silence.” The whistle-blowing revelations of Edward Snowden have broken this code of silence, and by so doing have alerted the general public to the widespread and intensive surveillance undertaken to protect them from terrorist attack. Widespread public concern over this surveillance has provoked the NSA to publicly declare the importance of such surveillance in terrorist plot interdiction.[208]

For companies that build terrorism risk models, this was something of a sea change. The radical transparency of Edward Snowden’s unlawful revelations may have provided sufficient information for the insurance industry to better understand the mitigation in place against the terrorist risk. But the shift is even more provocative.

According to Risk Management Solutions, terrorism risk can now be effectively modeled as a man-made catastrophe because, “Carriers writing terrorism cover are insuring against the failure of a government’s counter terrorism operations.” In short, the insurance industry is not ready to insure against terrorism. But perhaps they are ready to insure against the government failing to be successful.

This is a strange reorientation, and it highlights the various means available for dealing with the uncertainty associated with terrorist attacks. In the case of the UK reinsurance market it may indicate an important point of growth for the industry. Perhaps an improved ability for the insurance industry to work with security agencies within the UK will assist them in continuing to spread the risks of terrorism related losses and create viable markets, ultimately lowering the financial impact of terrorism, and perhaps even lowering the incentives of terrorism.

[208] Risk Management Solutions, *Quantifying U.S. Terrorism Risk*, White Paper (Newark, CA: RMS, 2014), 8.

Reinsurance, according to the Insurance Information Institute is “insurance for insurance companies.” Elsewhere it is more carefully defined as, “the insurance by an insurer of the liability of another insurer arising under contracts of insurance which the latter has entered into.”[209] Reinsurance functions as a global mechanism for transferring, sharing and profiting from the management of risks. Terrorism has proven to be an intractable risk—difficult to estimate both in terms of impact and probability, and thus difficult to establish viable rate setting measures, deductibles, and the other necessary apparatus of insurance schemes. From its inception, the UK government backed reinsurance program for terrorism risk was criticized as counterproductive. Critics argued that creating a government backstop for terrorism risk removed market incentives for private insurers to innovate ways to bear the cost of insurance, and felt that the scheme put in place was too onerous and costly to cultivate the growth of a viable market.[210] However, this most recent move towards private insurance (if only a single layer) may indicate a step in growth towards a viable private market for insuring against terrorism. Granted, it has taken more than two decades.

Little is publicly available about the precise decision making that led to commercial reinsurance for the Pool Re scheme. However, the purchase was brokered by Guy Carpenter, and provided by Munich Re.[211] Considering the enduring challenges inherent to modeling and insuring terrorism risk, the purchase of this reinsurance remains something of an enigma.[212] However, the connection between threat and intelligence analysis conducted by insurance firms and central to this brokered insurance sale may support the idea that the concept of reinsurance has changed somewhat in the UK, tying financial structures more closely to the work of counter terrorism and security agencies.

[209] William B. Bice, “British Government Reinsurance and Acts of Terrorism: The Problems of Pool Re,” *U. Pa. J. Int'l Bus. L.* 15 (1994): 441.

[210] Ibid.

[211] “Pool Re Purchases £1.8 Billion in Reinsurance,” PoolRe. Accessed March 9, 2015. https://www.poolre.co.uk/pool-re-purchases-1-8-billion-in-reinsurance/.

[212] See Guy Carpenter, *Global Terrorism Report,* (Chicago, IL: Marsh and McLennan Companies, 2014), and Risk Management Solutions, *Quantifying U.S. Terrorism Risk,* White Paper (Newark, CA: RMS, 2014).

Since its creation, the Pool Re scheme has paid for terrorism losses totaling £600 million across thirteen separate incidents.[213] In that time period UK insurance and government have had to respond to important changes in the insurance market and in the threats facing them. The availability of reinsurance on the commercial market has led some to question whether government programs are necessary as financial backstops to protect national economies from the impact of insurance companies withdrawing coverage and retreating from the market in the wake of attacks. Perhaps the reinsurance market at a state of maturity that it can effectively replace government programs to underwrite risk pools. The consensus appears to be that even with significant advances in modeling terrorism risk, the government must continue to provide some form of backstop.[214] The private industry, even with innovations in single layers of private reinsurance, is not robust enough to stand on its own.

2. Lessons for Unbounded Risk Management

The Pool Re scheme had to address the question of whether terrorism campaigns were to be a temporary disruption (e.g., an above average hurricane season or Northridge earthquake), or permanent change in conditions. This meant establishing a means of responding to changes in the threat paradigm, and evolutions in the insurance market.

Evolutions in insurance provide useful lessons for how homeland security agencies might approach unbounded risks. In its essence, insurance is fundamentally about the management of uncertainty. However, there are evidently risks which are either too uncertain or with losses too concentrated or catastrophic for insurance to devise a profitable actuarial model for them. The necessary components for transforming raw uncertainty into rational risk are insufficiently available for private sector insurance to effectively manage them alone. In such cases, the risks are often shared with the government, or managed through risk pools. The insurance of flood risk, nuclear reactor risk, and insurance against terrorism each illustrate the way that the private sector and the

[213] "Pool Reinsurance Company Ltd.," PoolRe. Accessed March 14, 2015. https://www.poolre.co.uk/.

[214] Guy Carpenter, *2015 Terrorism Risk Insurance Report*, Insights, (Chicago, IL: Marsh and McLennan Companies, June 2015).

government have worked together to provide insurance against particularly challenging uncertainties. In particular, governing terrorism risk through insurance has evolved and is beginning to show signs of developing out of temporary programs and towards a private market capacity to take on a larger share of the risk. However, it seems unlikely that terrorism risk will ever be fully taken back by the private sector. And this may offer some lessons about the enduring character of the uncertainty in play.

Insurance does not prevent loss. It is not, by itself a counterterrorism or counter catastrophe strategy, but a mitigation measure. It ensures that losses can, in some way, be compensated. Reducing the cost and consequence of catastrophe does not undo the loss of life, or prevent the terrorist attack from happening, but it does promise a measure of control. It may even reduce the incentive for terrorism by demonstrating to the terrorist that their actions may result in loss, but not devastation.[215] It may reduce the element of terror that the terrorist pursues. Considering the dimensions of risk, insurance does not alter the threat (probability), but mediates the consequence by reducing vulnerability.

The profitability of insurance or the extension of credit depends on selecting risks, and establishing corresponding actuarial rates, deductibles, etc., in order to both compensate the loss, and run at a profit. Critiquing Beck's Risk Society thesis, insurance analysts have argued that, "insurers have always been selective about the risks they assume...some risks that have proven too difficult to insure in the private market – for example, the risk of unemployment or of flooding in specific regions – are addressed by government insurance schemes. Other such risks are not insured at all."[216]

Homeland security agencies do not have such free market luxuries. Laws that require homeland security agencies to manage risks that the private sector has abandoned due to their uncertainty or concentration present a problem of inherently unbounded risk.

[215] I rely here on Bruce Hoffman's definition of terrorism, which includes a prerequisite for a political end achieved through violence or the threat of violence. If violence is increasingly compensable, then the terrorist will face an obstacle in achieving influence. See Bruce Hoffman, *Inside Terrorism* (New York, NY: Columbia University Press, 2013), 40.

[216] Richard Ericson and Aaron Doyle, "Catastrophe risk, insurance and terrorism," *Economy and Society* 33, no. 2 (2004): 135-173.

Evaluating the National Flood Insurance Program (NFIP) after Hurricane Katrina, the American Institutes of Research noted that, “Because flooding is unpredictable and catastrophic in nature, only those most at risk would be likely to purchase the insurance, precluding the accumulation of funds sufficient to cover claims that would have to be paid. This phenomenon is known as ‘adverse selection’ and is inconsistent with a sound private insurance program.”[217] The problem of adverse selection was part of the genesis of the NFIP. As construction near water expanded the profile of flood risk in the nation, the NFIP was established as a means of reducing dependence on federal disaster relief and decreasing the consequences of flood through a national risk management and insurance program. Likewise, since 1957, claims resulting from nuclear reactor accidents have fallen under the Price-Anderson Act. Nuclear reactor risk is addressed through a primary tier of industry insurance for each reactor site, and a second tier industry-wide pool that contains more than $12 billion in funds.[218] Congressional disaster relief would address losses exceeding $12 billion.[219]

The result, according to Richard Ericson and Aaron Doyle is a symbiotic relationship between government security entities and private sector insurance to provide against unbounded risks:

> This is a story of how, in conditions of extreme uncertainty, insurers have difficulty forming a market, and seek the help of governments as the insurers of last resort. Governments, meanwhile, seek both the capital and preventive security capabilities of the insurance industry to spread at least some of the risk.[220]

This theme has been picked up by others as a critique of Beck’s view of unbounded risk. Claudia Aradau and Rens Van Munster contend similarly that

[217] American Institutes for Research, *The Evaluation of the National Flood Insurance Program Final Report* (Washington, DC: October, 2006), 2.

[218] United States Nuclear Regulatory Commission, “Backgrounder: Nuclear Insurance and Disaster Relief” (Washington, DC: June, 2014).

[219] “An Act to amend the Atomic Energy Act of 1954, as amended, and for other purposes,” Public Law 85-256, September 2, 1957, and “The Energy Policy Act of 2005,” Public Law 109-58, August 8, 2005.

[220] Ibid.

unbounded risk has engendered new and creative responses that combine the capabilities of government institutions charged with the provision of security and private sector institutions capable of capitalizing on risk:

> The argument that catastrophic terrorism is incalculable and uninsurable appears therefore inattentive to the institutional measures and actions that surround the tragic events of 9/11. Against the backdrop of radical contingency and incalculability, institutions have attempted to devise means to minimize or avoid the catastrophic promise of the future, seeking for alternative ways to predict and master it.[221]

Like the prospect of risk-based security, this has an immediate appeal. The joint efforts of institutions of government and insurance may represent an ability to adapt to changing risks rather than signaling a new character to risk that defies insurability altogether. In this way of thinking, Beck is giving insufficient credit to the breadth and complexity of the insurance response to high uncertainty or catastrophic possibility. Governments can underwrite unbounded risks, and insurers can help spread them.

Terrorism's adaptive uncertainty makes it extremely difficult to tame and take chances. It is only possible to manage terrorism through the paradigm of insurance by creating a monetary fortress in the form of government underwriting. This joint arrangement between private and public sectors is as complex as Beck's critics claim, but perhaps as tenuous as Beck feared. The solidity of the arrangement might be dissolved by a catastrophe beyond our current imagination.

E. CONCLUSION: THE WILDERNESS OF RISK

Normal accidents, worst cases and the risk society bring with them unseen connections, improbable consequences, and a landscape of insecurity and uncertainty.

The growing awareness of risk possibilities that are less and less responsive to the measures we have in place presents a challenge for homeland security. Risk controls and procedures established for a rail transport system—from the design of rail cars to the

[221] Claudia Aradau and Rens Van Munster, "Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future," *European Journal of International Relations* 13, no. 1 (2007): 89–115.

procedures for checking brakes—are still designed in isolation. A fireman cannot forecast the impact on braking measures of shutting off a locomotive engine. And yet, the worst case, the possibility resulting from this oversight is not a peripheral issue, but, when illuminated by catastrophe, the principal concern of homeland security agencies.

In hindsight, the Lac-Mégantic rail accident does not look inexplicable. Indeed, in the clarity of hindsight it takes on the appearance of inevitability and calculated certainty as we observe the alignment of risks.

The risks that homeland security agencies face remain especially resistant to risk management methods. And this may be the true utility of Ulrich Beck's claims concerning risk society—not that risk analysis is never useful, but that risks in the modern era increasingly amplify uncertainties. This has profound implications for the way that organizations should respond to them.

Even something as prosaic as a multi-jurisdictional watershed illustrates the how risks can be unbound, even when well understood. Increasingly dense communities and infrastructures that transect jurisdictional boundaries, professional disciplines, and social vulnerabilities combine in unforeseen and unperceivable ways. The cause and the effect of risks are separated, and occluded for the analyst.[222] For those who would presume to design measures to control such risks, the possibility of exploiting chance is diminished because it is increasingly impossible to have the full picture of data necessary to calculate either the possibility of a bad thing happening, or the forms that bad thing might take. Social amplification, catastrophic possibility, and the elongation and permanence of losses defies the homeland security agency seeking to organize its effort around precisely the things it finds it cannot know.

This chapter concludes with a troubling thought. If we can admit to the dimensions of contemporary risk, what arrangements ought we to have in place for

[222] For example, while the FEMA Risk Mapping, Analysis and Planning program is increasingly including watershed level assessments of flood risk, regulatory products developed under the NFIP are still approved at the jurisdictional level. Non-regulatory products that take a broader view support more comprehensive planning, but the flood studies conducted to calculate discharge rates and establish regulatory floodways and floodplains are conducted, by necessity, on a narrow scale.

confronting this deep and expanding uncertainty? As the future acquires new dimensions of inscrutability, what impact should this have on the plans of the present? Chapter 3 will argue that our doctrine, and organizational arrangements largely commit a surprising error: treating the uncertainty that dominates the responsibilities of homeland security with tools better suited to reliable, predictable, rational futures.

III. UNCONSCIONABLE MAPS

Unconscionable, a. (sb., adv.)...
b. Unreasonably excessive.

—*Oxford English Dictionary*

1. The map is not the territory.
2. The map represents not all the territory.
3. The map is self-reflexive.

—Alfred Korzybski[223]

Unconscionable maps do not know they are maps. They are maps that have forgotten they are not the territory, which believe they represent all the territory. They are the thousand page operational plan that remains unread by the first responder, or the unattainable presumption to a national, “near real-time situational awareness capability” for threats and hazards.[224] They are measured as unreasonable or excessive not by being false, but by being incomplete and unaware of themselves.

In this chapter, I will consider the ways that homeland security has responded to unbounded risk. Largely, this response has been the creation of unconscionable maps. The security response to unbounded risk often displays two problematic tendencies: the pretense of applying risk management when the information necessary to support such calculation is not available, and boundless precaution. In the first case homeland security lives with a false assumption that it has exerted control over a risk, in the second, homeland security has little assurance or measure of success and surrenders decisions to threat politics.

[223] Alfred Korzybski, *Collected Writings, 1920-1950*, Edited by M. Kendig (Fort Worth, TX: Institute of GS, 1990), 205.

[224] White House, *Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience* (Washington, DC: White House, February 12, 2013).

Homeland security is promising and pursuing greater security than it can achieve. In the process, it is making unconscionable maps. Unbounded risk further makes it difficult for what have become standard homeland security practices to produce anything other than unconscionable maps.

The doctrines, depictions, plans and tools in place for managing unbounded risks are arguably extensions of what curator Robert W. Karrow Jr. describes as a "mapping impulse"—the creative disposition to explain one's place in the world.[225] Defining just what a "map" is has become, according to Karrow, "a rather contentious issue in the field."[226] Karrow describes the way that, "Administrators and politicians 'map strategy,' teachers use an 'english curriculum map,' and diplomats follow a 'roadmap toward peace."[227] Homeland security has its own maps too. In homeland security, the noun "map" and the verb "mapping" encompass visual representations and abstractions from regulatory maps displaying the various characteristics of special flood hazard areas, to catastrophic plans and concepts of operation. For this reason, Karrow proposes the broader concept of a "mapping impulse" that speaks to a desire to find one's place in the world. Such wayfinding maps, says James R. Akerman, "do not just tell us where we are going, they also tell us who we are."[228]

All maps are abstractions. They are not the thing they represent, but are instead an explanation of it, an orientation or a statement of relationship to it. Maps are not just spatial navigational tools, they express a range of data, intended use, and even self-conception and belief. Certain Japanese pilgrimage maps from the Edo period are not laid out by distance, but by devotional activities to be performed at key shrines. London underground maps from the 1920s are not geographically accurate, but represent an equal

[225] Ibid., 19.

[226] James R. Akerman, and Robert W. Karrow, *Maps: Finding Our Place in the World* (Chicago, IL: University of Chicago Press, 2007), 1.

[227] Ibid., 9.

[228] Ibid., 19.

distance between stations. Underground, the distance between stations is not the important thing, simply the station name.

What should homeland security professionals make of the Nuclear/Radiological Incident Annex to the National Response Framework?[229] This is a map. It is a practical tool designed to orient action and explain the purpose and function of security measures. Such maps are used in proverbial briefings and in accounting for action to appropriations and oversight committees in congress. They are practical culture. But they are also semantic, rhetorical culture. They explain homeland security to itself and others.

In chapter two I argued that the homeland security risks America faces are progressively beyond our capacity to perceive, prevent, or control them. This puts considerable strain on the common concept that homeland security must be risk-based. Even in areas where we have sophisticated measures in place, the most prosaic and well understood of hazards still defy us. We cannot rule out even flood disaster, where decades worth of data and refined analysis allow us to develop detailed regulatory risk products around floodplains.[230]

In this chapter I consider the way that homeland security lives with such possibilities. I will argue that homeland security theory and practice has insufficiently addressed uncertainty. Not through inaction, but through action ill-suited to the changing nature of risks. Domestic security efforts are pursuing certainty where they cannot have it, and disguising enduring uncertainty with boundless precaution. Where risk was designed as the exploitation of chance, many of the central arrangements in place for providing domestic security deny or seek to eliminate chance. Here risk management becomes a means of eliminating waste and increasing efficiency. Noble ends, but ends not aimed at the unthinkable, or the worst case.

[229] FEMA, *Nuclear/Radiological Incident Annex* (Washington DC: 2008), and “Layers of Security,” Transportation Security Administration, Accessed June 12, 2015, http://www.tsa.gov/about-tsa/layers-security.

[230] Federal Emergency Management Agency, *FEMA P-765, Midwest Floods of 2008 in Iowa and Wisconsin, Mitigation Assessment Team Report* (Washington, DC: FEMA, 2009).

"For more than six decades," says sociologist Robert Wuthnow, "humankind has lived with knowledge that it could be the agent of its own annihilation."[231] He is referring, of course to the advent of nuclear technology. As Wuthnow assesses in his book *Be Very Afraid*, our response to such knowledge has not been the paralysis of fear, or the mad rush of panic, but a complex, and essentially human network of disciplined action. As we become acquainted with terrible possibility, from terror to pandemics, we have done a great deal to secure ourselves against a variety of doomsdays. We have not responded to unbounded risks with inaction, quite the contrary. The changing nature of risks has had a dramatic impact on our arrangements. 9/11 introduced the idea that catastrophic terrorism, even as an outlier, was a possibility. In the same way, our heightened awareness of abstruse and apocalyptic hazards has imprisoned security agencies between paralysis and precaution. Faced with an expanding menu of possibility, high uncertainty and catastrophic potential, the predominant mode of action has been an abundance of caution. Such precaution costs money. Expenditures on domestic security have increased over $1 trillion in the last decade.[232] Treating Ebola in the United States cost over $1 million per patient, and in Africa alone could cost $15 billion over the next five years.[233] Unbounded risk makes it very difficult to discern how much security is enough, or to measure the effectiveness of the measures we have. Unbounded security measures lack a limiting principle. And, paradoxically, such precaution may be making us less secure.

[231] Robert Wuthnow, *Be Very Afraid: The Cultural Response to Terror, Pandemics, Environmental Devastation, Nuclear Annihilation, and Other Threats* (New York, NY: Oxford University Press, USA), 2010.

[232] John Mueller and Mark Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (New York, NY: Oxford University Press, USA, 2011), 3.

[233] Statement of Chancellor Jeff Gold, M.D. University of Nebraska Medical Center, Omaha, Nebraska before the Committee on Energy and Commerce Subcommittee on Oversight & Investigations Hearing on "Update on U.S. Public health Response to Ebola Outbreak" United States House of Representatives 113th Congress November 18, 2014. See also United Nations Development Group. *Socio-Economic Impact of Ebola Virus Disease in West African Countries: A call for national and regional containment, recovery and prevention*. New York, NY: United Nations Development Group—Western and Central Africa, February 2015.

Unconscionable maps have a tendency to pave over uncertainty—to render organizations insensitive to it. Homeland security maps often presume control over things we cannot control. This presumption of control is manifested in our doctrines, our organizational arrangements, and the way that aspiration and practice confront threats and catastrophes through plans and operations. In *Mission Improbable*, Lee Clarke examined the way that organizations often respond to situations that defy, "operational rationality,"[234] that is, situations where the organization lacks sufficient information to produce a plan that mirrors reality. In such situations, organizations often produce what Clarke calls "fantasy documents." Such documents do not actually guide operations, but rather serve as reassurances that the organization has taken the problem seriously and stands ready to deliver. Such plans are symbolic, not real.

In unbounded risk, however, homeland security is unable to know or estimate significant details of that risk. Methods designed for bounded problems may not be suited to unbounded problems. Organizational approaches designed to produce efficiency depend on a regular landscape, in the same way that a factory might optimize production based on known and maintained stasis in a production environment. But homeland security risks do not hold still, and models designed for efficiency permit an illusion of control in the face of changing environments. In this case an unconscionable map presumes or pursues that which it cannot have. In making such pursuit the central concern of much homeland security planning, doctrine and practice, security organizations are, in turn, poorly situated to confront uncertainty.

In chapter two I contended that risks are outpacing the pursuit of control. In this chapter, I will consider the way that domestic security is arrayed against this reality in four categories of unconscionable maps:

- Precaution
- Plans, Atlases and Threat politics
- National Incident Management Uniformity
- Command and Control

[234] Clarke, *Mission Improbable*, 73.

A. HERE BE DRAGONS: PRECAUTIONARY MAPS

> *Imagination is not a gift usually associated with bureaucracies...It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination. Doing so requires more than finding an expert who can imagine that aircraft could be used as a weapon.*
>
> —9/11 Commission Report[235]

> *Zhuping man studied the art of butchering dragons under Crippled Yi. It cost him the thousand pieces of gold he had in his house, and after three years he had mastered the art, but there was no one who could use his services.*
>
> —Zhuangzi[236]

The bureaucratized imagination is surprisingly vivid. Of the fifteen National Planning Scenarios designed in 2005 to support the implementation of HSPD-8, twelve were terrorism related. They included blister agent chemical attacks and improvised nuclear devices, but excluded the threat of electromagnetic pulse weapons.[237] In 2014, H.R 3410 set about to correct this oversight.

The draft Critical Infrastructure Protection Act or CIPA, which passed the house in 2014, would, "require the Assistant Secretary of the National Protection and Programs Directorate to: (1) include in national planning scenarios the threat of electromagnetic pulse (EMP) events."[238] Apparently unbeknownst to the authors of H.R 3410, the national planning scenarios were rescinded in 2011 with the institution of PPD-8, which replaced HSPD-8. This detail would make H.R 3410 either very easy, or very difficult to implement if it were to pass the senate. The authors of the bill might be forgiven for

[235] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, NY: W.W. Norton & Company, 2004), 344.

[236] Zhuangzi, *The Complete Works of Zhuangzi*, translated by Burton Watson, Translations from the Asian Classics (New York, NY: Columbia University Press, 2013), 281.

[237] Homeland Security Council, *National Planning Scenarios: Executive Summaries Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities* (Washington, DC: Homeland Security Council, April, 2005).

[238] H.R.3410-Critical Infrastructure Protection Act, 113th Congress (2013-2014).

missing such an arcane detail (though perhaps lawmakers should know better). But scenarios are a persistent fixture in homeland security's pursuit of organizational, bureaucratic imagination. H.R 3410 presents a problematic reminder that it is possible to invest in a single uncertain risk at the exclusion of other risks. The bureaucratized imagination can, perhaps, hyperextend itself, or come to believe in itself too much. Homeland security organizations should be wary of the lesson of Zhuping man, who gave his fortune to prepare to fight a dragon, only to find himself in a world without dragons.

The saying was proverbial as early as 1934, that generals are always ready to fight the last war.[239] But the alternative offers no easy solutions. How should homeland security prepare to fight the next war, thwart the next attack, or respond to the next catastrophe? By now these questions are also proverbial. *The 9/11 Commission Report* admonished the Federal government's insufficient imagination.[240] According to *The 9/11 Commission Report*, the intelligence, law enforcement, and domestic security and preparedness apparatus of the nation failed to credibly imagine the possibility of an aircraft used as a weapon. The mirror twins of failing to take action against a catastrophic possibility are to give credulity to every imagined possibility, or to suppose you are able to imagine every possibility.

So it is challenging to parse out just what the failure of imagination consisted of, if indeed *The 9/11 Commission Report's* charge of failure is to stand. *The 9/11 Commission Report* is not merely arguing that agencies failed to think of an outlandish counterfactual, but that they failed to take it seriously. According to the report, they failed to take action against it. In 1945 B-25 bomber crashed into the Empire State Building. In the years before, Japanese Kamikaze attacks demonstrated the effectiveness of using aircraft as weapons.[241] *The* 9/11 *Commission Report* identifies that security concerns and

[239] Edward P. Warner, "Present Conditions under the N.R.A" *American Marketing Journal* Vol. 1, No. 1, January (1934), pp. 6-14.

[240] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, NY: W.W. Norton & Company, 2004), 344.

[241] Clarke, *Worst Cases*, 91.

exercises had already considered the counterfactual that an aircraft might be used as a weapon.[242] For the exercise of imagination this is troubling. As the report argues, America needs something more than an expert capable of imagining such things. It wants for something more than planning scenarios.

"Generally speaking," argues Erwan Lagadec, "in all countries and sectors, [leaders] have proved culturally incapable of taking the 'unthinkable' seriously, let alone react effectively when it actually occurred."[243] What, then, is the appropriate organizational response to the unthinkable? In evaluating the reaction to 9/11, it is likely that the purpose of bureaucratized imagination, and even the purpose of scenarios must be something more than simply preparing for that scenario.

There is, it seems an intrinsic value in cultivating the exercise of imagination. In cultivating our ability as organizations to take the unthinkable seriously and to expect the impossible. In pondering such matters the American response has been the embrace of precaution. This may be an unsuitable form of imagination.

1. The Precautionary Principle

To avoid potential injury…

—Safety signage from a shopping cart

The precautionary principle is often expressed as an idiom: better safe than sorry.[244] The principle, "counsels that we should avoid steps that will create a risk of harm; until safety is established through clear evidence, we should be cautious."[245] In a more detailed sense the precautionary principle proposes that in situations with limited information or confirming fact, "in the absence of scientific near-certainty about the

[242] Ibid. 92.

[243] Erwan Lagadec, "Unconventional Crises, Unconventional Responses: Reforming Leadership in the Age of Catastrophic Crises and Hypercomplexity," *Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies* (Baltimore, MD: Johns Hopkins University, 2007).

[244] Sunstein, *Laws of Fear: Beyond the Precautionary Principle*, 224.

[245] Cass Sunstein, "The Paralyzing Principle," *Regulation* 25, no. 4 (Winter 2002/2003 2002): 32.

safety of the action, the burden of proof about absence of harm falls on those proposing the action."[246] From a regulatory standpoint this could mean prohibiting or limiting actions which have not been proven to be safe, but precaution can also reflect a bias for action, particularly when homeland security organizations take precautionary measures against threats and hazards that are uncertain. A precautionary stitch in time saves nine. Often, such precaution lacks a limiting principle. Avoiding injury is insufficient, it seems. We must also avoid the potential for injury.

Cass Sunstein has examined some further problems with the precautionary approach. Taken seriously, says Sunstein, the precautionary principle would in fact be a "paralyzing principle"—as any action designed to address one risk would bring with it potential risks and uncertainties.[247] But the precautionary principle has come to represent a dominant force in thinking about uncertain risks, particularly at the regulatory level, and particularly in the European Union.[248] It is not difficult to see why. The motivation behind precaution is noble, an approach intended to oppose undesirable possibilities, without delaying unnecessarily.

In contrast to precaution, John Rawls "maximin principle" argued that in conditions of uncertainty, we ought to rank alternatives by their worst possible outcomes, and select the outcome with the best worst case.[249] Refining the thinking of Rawls, Sunstein proposes an "anti-catastrophe principle" as an antidote to the paralysis of precaution.[250] Sunstein's view is that the precautionary principle is, "literally incoherent," preventing organizations from deciding whether the risk they are addressing is more problematic than the risk of taking action against it or neglecting one risk in favor

[246] Nassim Nicholas Taleb, et al., "The Precautionary Principle (with Application to the Genetic Modification of Organisms)," *Extreme Risk Initiative* (New York, NY: NYU School Of Engineering Working Paper Series, September, 2014).

[247] Ibid.

[248] Ibid., 17.

[249] John Rawls, *A Theory of Justice* (Boston: Harvard University Press, 2009), 133.

[250] Sunstein, *Laws of Fear: Beyond the Precautionary Principle*, 224.

of another.[251] For instance, Sunstein favors a “rule utilitarian” ban on torture over a moral heuristic, as he feels that a moral heuristic will predictably misfire. Selecting the rule utilitarian approach does not argue that torture could never be justified, but that unless it is wholly outlawed, governments will resort to torture in situations where it is not justified. Granting the permission to torture in extraordinary cases will, from this second order perspective do more harm than good.[252] This may be taken as regulatory philosophy—that the government has a responsibility to the address and take action against the worst aspects of worst cases. Both Sunstein and Rawls present more conservative, targeted approaches to uncertainty that embrace the possibility of catastrophe, but do not surrender to boundless fear.

Precaution, says Sunstein, results it a, “selectivity of fear.”[253] This means fearing only those threats that are prominent or available. Such availability is subject to the influence of media coverage, etc. Precaution then puts risks in the hands of political will, not probability. Unbounded risk presents a hurdle to this problem. As we have seen, unbounded risk is problematic because it prevents the assignment of probabilities in some cases. In such situations, Sunstein argues that the anti-catastrophe principle is a more useful tool than the precautionary principle, limiting governmental action to the worst of the worst cases and constraining the tendency toward boundless imagination or political advocacy for specific threat prominence.[254]

2. Precautionary Mappaemundi

Medieval mappaemundi were typically tripartite or T-O maps, so called because they depict the Mediterranean, the Nile and the Tanais as dividing Europe, Asia and Africa (the T), all surrounded by a circumfluent ocean (the O).[255] These were maps of the

[251] Ibid.

[252] Ibid., 217.

[253] Ibid., 24.

[254] Ibid., 109.

[255] Chet Van Duzer, *Sea Monsters on Medieval and Renaissance Maps*, 14

world in its entirety, enclosing all that mattered within a ring of ocean. The mapping impulse evident in these mappaemundi reflects a pursuit of bounded certainty, circling that which is important and pursuing greater knowledge within.

Worst-cases and unbounded risk invite a tendency toward precaution, and precaution invites a tendency to pursue omniscience. "Terrorism," says Claudia Aradau and Rens Van Munster, "is to some extent a 'risk beyond risk', of which we do not have, nor cannot have, the knowledge or the measure."[256] Unbounded risk presents difficulties to such conceptions of the world for homeland security. Says Claudia Aradau, "although Beck presents risk society as riddled with risks of which we can have neither knowledge nor measure, the 'war on terror' displays an insatiable quest for knowledge: profiling population, surveillance, intelligence, knowledge about catastrophe management, prevention etc."[257]

The governmental appetite for precautionary information is the result of confronting such challenges. Bulk data collection conducted through the National Security Agency reflects an understandable extension of both precautionary philosophy and the challenges of unbounded risk and pervasive uncertainty. In a security environment characterized by uncertainty, where what agencies and organizations do not know becomes more important than what they do know, the collection of all information, even irrelevant information, appears a necessity. In such uncertainty, "the traditional technologies of risk management become more extensive, as profiling and surveillance attempt to encompass the whole population."[258]

In precautionary data collection and analysis, the management of uncertain risks like terrorism becomes less about confronting specific threats that currently exist, and increasingly about the anticipation and prevention of an infinite array of possible futures. In this case, "the rationality of catastrophic risk translates into policies that actively seek

[256] Claudia Aradau and Rens Van Munster, "Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future," *European Journal of International Relations* 13, no. 1 (2007): 89–115.

[257] Ibid.

[258] Ibid.

to prevent situations from becoming catastrophic at some indefinite point in the future."[259] The ongoing debate and legal determination about the government's ability to collect, for instance, phone data about American citizens that it does not currently need, but might eventually need to support intelligence analysis and counterterrorism is the formalization of government precaution.[260] It is difficult to understate the shift contained in this approach to security. Where risk arose out of a desire to tame chance and take calculated risks, precautionary security is more fundamentally fearful.

In an occasional paper written for the Central Intelligence Agency's Sherman Kent Center for Intelligence Analysis, Jack Davis considered a troubling question. If surprise is inevitable, what could be the role for intelligence analysis? He frames his argument with an axiom: "If surprise can succeed despite robust tactical warning, then defense must utilize effective strategic warning to prepare to succeed despite surprise."[261] Davis acknowledges that the catastrophic surprise of 9/11 colors the thinking in his paper, and informs his recommendations. As argued by Davis, the United States must, "reconstitute strategic warning analysis as a collaborative governmental responsibility," as opposed to a function consigned to intelligence alone. This conclusion mirrors the conclusion of the *9/11 Commission Report* that called for renewed strategic analysis capacity.[262] But Davis examines further the nature of strategic intelligence as opposed to tactical intelligence and the connection between analysts and policymakers who make use

[259] Ibid. The case made in this paper is the need to acknowledge that the way in which modernity has responded to risk society has been to aggressively deploy many different means of exerting control over catastrophic possibility. This has meant dramatic expansion in capability, and attempts to debound security to match unbounded threat. This hardly undermines the idea of risk society, but it recognizes and aggressive posture in confronting the reality of risk society.

[260] Savage, Charlie, "Surveillance Court Rules That N.S.A. Can Resume Bulk Data Collection," The New York Times, June 30, 2015. http://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html.

[261] Jack Davis, "Strategic Warning: If Surprise is Inevitable, What Role for Analysis?" *The Sherman Kent Center for Intelligence Analysis,* Occasional Papers: Volume 2, Number 1 (Washington, DC: January 2003).

[262] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, NY: W.W. Norton & Company, 2004), 404.

of analysis. It is a paper fitting for the Sherman Kent center, reminiscent of Kent's own quip that the purpose of intelligence analysis was to, "elevate the quality of discussion in this town."[263]

Davis is not optimistic about relying too much on tactical—credible and immediate—warning. He is confident that we will be surprised. But, while Davis is concerned that, "these and related analytic skills for disciplined assessments of seemingly unlikely dangers are key to distinguishing strategic warning analysis from exercises in worst-case speculation," it remains unclear whether such, "disciplined assessment," can really provide any antidote to precautionary information collection and analysis.[264]

Precautionary data collection is part of a broader security mapping impulse toward perfect knowledge. Fundamentally uncertain risk understandably results in the sustained impulse and pursuit of more knowledge about threats and hazards in order to close the gap. But it is difficult to know when enough information has been collected, or to assess how much that information reduces the risk or allows for control over danger.

Presidential Policy Directive 21: Protecting Critical Infrastructure, put forward a national goal of "near real-time situational awareness" of threats and hazards to critical infrastructure.[265] On the face of it this may seem a remarkable assertion and goal. Such knowledge is unattainable even at the facility level in many locations and industries. The pursuit of such absolute knowledge of threat, hazard and system has built an entire industry of dashboards and viewers, geospatial platforms and catalogues of risk assessments. Homeland security organizations and agencies have, in large part, cohered around methods for accumulating and sorting through such information.

[263] Jack Davis, "Sherman Kent and the Profession of Intelligence Analysis," *The Sherman Kent Center for Intelligence Analysis*, Occasional Papers: Volume 1, Number 5 (Washington, DC: November, 2002).

[264] Ibid.

[265] White House, *Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience* (Washington, DC: White House, February 12, 2013).

Claims to national "near real time" knowledge are in this sense unremarkable. They are supported by the large-scale organizational pursuit of those ends. Data collection and domain awareness do not necessarily suppose that all information can be known, but they have as their animating principle the idea that the more unlimited information collection capabilities and pursuits are, the better security will be. Unbounded risk challenges this assumption with the idea that the information necessary to avert catastrophe will, by definition, only be revealed in catastrophe.

Even in our current environment of relatively boundless precaution, the principle of unbounded risk argues that we cannot rule out catastrophe. In such a universe, it is difficult to argue that precautionary collection has delivered security.

3. Precautionary Amplification of Risk

The Professor, Joseph Conrad's nihilistic, bomb making villain in *The Secret Agent*, walks the streets of London with a flask filled with high explosives that he can detonate within 20 seconds. As a result, the authorities give him a wide berth. Explains the professor:

> I have the means to make myself deadly, but that by itself, you understand, is absolutely nothing in the way of protection. What is effective is the belief those people have in my will to use the means. That's their impression. It is absolute. Therefore, I am deadly.[266]

Political writer Paul Berman complains that Conrad's terrorists are, "marginal screwballs." To his thinking, Conrad wasn't taking anarchists and nihilist "death cults" seriously enough.[267] Jack London's 1907 fictional terrorist Emil Gluck is probably more to Berman's liking, as a "nihilist, or annihilist" who first murders those close to him, then expands to terrorism against military, police, royal, and ultimately random targets before inventing a machine that allows him to exterminate tens of thousands.[268] But Berman

[266] Joseph Conrad, *The Secret Agent: A Simple Tale* (New York, NY: Doubleday, Page & Company, 1916), 80.

[267] Paul Berman, *Terror and Liberalism* (New York, NY: W.W. Norton & Company, 2004), 36.

[268] Jack London, *The Strength of the Strong* (New York, NY: Macmillan, 1914), 101.

seems to miss that *The Secret Agent* is a satire about England's counterterrorism efforts. For Conrad, the government response to terrorism posed a greater danger to liberal society than a bunch of screwball anarchists who wanted to blow up the Greenwich Observatory. So he satirizes the external threat to highlight the danger of a self-inflicted threat. Believing in the danger posed by the Professor caused a corresponding restriction of liberty. The source of the Professor's power lies with the way he is perceived, not the means at his disposal. The 9/11 Commission concluded that the Government did not take its imagination seriously enough. Conrad warns against the dangers of taking it too seriously.

It is difficult to balance such concerns. What threats and catastrophes must homeland security take seriously, and what actions must security organizations take against them? How can the perception of danger impact, amplify and legitimate the danger itself?

In Conrad's Professor, we can see the roots of Barry Buzan's "securitization"—framing issues as security problems.[269] Buzan ably captures the dimensions of efforts to problematize in the context of security, but what does this process mean for the security imagination? Securitization contains a transformative power, able to transform both bridge and carnival equally into the language of vulnerability, susceptibility, target selection and impact assessment.

German photographer Simon Menner captured this transformative power in a recent photograph exhibit entitled "Camouflage." Working with the German Army, Menner photographed woodland landscapes where snipers had concealed themselves.[270] The resulting images are unsettling. The effect of knowledge on the viewer (knowing that a threat is concealed in the nature scene) invites a sense of foreboding. Menner's photographs either transform nature to a wilderness, or serve as a reminder that it was

[269] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998), 23.

[270] David Rosenberg, "Camouflage is a Conceptual Look at Snipers," *Slate Magazine*, New York, January 20th, 2015.

always wild. They are reminders of lurking danger, but also lessons in the way that securitization can amplify fear, and alter perception.

The way that organizations perceive and respond to a risk can present its own risk—if, for instance surveillance programs infringe upon privacy rights. Such organizationally amplified risks provide several important observations about the way that homeland security organizations ought to process and respond to fear. Sociologist Robert Wuthnow has assessed that rather than reacting to fear with paralysis, humans have a, "bias for action" in the face of fear.[271] But this tendency, says Wuthnow, to do something about fear is not a mindless or reflexive response, but a mentally engaged one as well. In Wuthnow's observations there lies the crucial consideration of just how readily fears reflect reality. The psychological heuristics, or methods of thinking that Daniel Kahneman considered in *Thinking, Fast and Slow* illustrate powerfully the way that particular patterns and tendencies influence the way that humans respond to facts, often making poor decisions based on an autonomic tendency to substitute simpler problems for more complex ones, favoring reaction over contemplation in many cases.[272]

Such heuristics, and the possibility for the social amplification of risk indicate a grave responsibility on the part of homeland security organizations to respond to risk effectively. This is a more complicated business than simply elevating or decreasing the volume of official fear around a given subject, but requires an approach tailored to the reception of the information. Smokers, for instance, tend to overestimate the health risks of smoking...but smoke anyway. In such cases the appropriate response in terms of risk communication would not be to focus on communicating how bad the risk of smoking is—since smokers have already demonstrated a form of immunity to such information.[273]

[271] Robert Wuthnow, *Be Very Afraid: The Cultural Response to Terror, Pandemics, Environmental Devastation, Nuclear Annihilation, and Other Threats* (New York, NY: Oxford University Press, USA, 2010), 214.

[272] Daniel Kahneman, *Thinking, Fast and Slow* (New York, NY: Doubleday, 2011), 44.

[273] Paul Slovic, *Smoking: Risk, Perception, and Policy* (London, UK: SAGE, 2001), and Kip Viscusi, *Smoking: Making the Risky Decision,* (Oxford, UK: Oxford University Press, 1992).

Organizations must make similar decisions in considering which risks to take action against, and what action to take. If the degree of dread, political visibility, or media saturation around a certain risk drives such decisions, organizations are in a position of surrendering the analysis of risk to the perception of risk. All risks then present dual dangers. They are both the dangers they pose, and the dangers of our reactions to such information. Here the failure of imagination returns with equal duality. The way that security organizations respond to possibility presents the potential to amplify risks. The bureaucratized imagination can be dangerous.

The United States spends more than $16 billion annually on counterterrorism efforts within the U.S. intelligence community alone.[274] This does not account for the amount spent on other counterterrorism efforts within DHS and elsewhere. Such spending is almost certainly too much, too little, or just the right amount. Uncertainty and volatility make it difficult to make sense of a number such as this.

Our spending on counterterrorism is largely precautionary spending, meaning it cannot be accounted for through actuarial means or cost-benefit analysis. The homeland security enterprise will always be in danger of veering one way or the other; surrendering hazard specific priorities to horrific possibilities, or ignoring the possible and focusing only on probabilities and controllability.

B. PLANS AND ATLASES

Plans are expressions of how to achieve a stated end. If the plans that homeland security produces are unconscionable maps, then it is due in part to planning methodology. Planning in conditions of uncertainty means that at least part of the challenge of the plan is how to make sense of organizing people and things to achieve an end, when operating conditions and even desired ends may change without warning.

[274] Drew DeSilver, “U.S. Spends over $16 Billion Annually on Counter-Terrorism” Pew Research Center. Accessed July 4, 2015. http://www.pewresearch.org/fact-tank/2013/09/11/u-s-spends-over-16-billion-annually-on-counter-terrorism/.

The dominant methods of security planning have grown up around such uncertainties. Planning methodologies are, in some important ways, means of reducing uncertainty while still taking action. Two planning methods in particular have come to characterize national preparedness planning efforts: scenario planning, and capabilities-based planning. Each method proposes a different approach to address and ostensibly reduce the problem of uncertainty.

However, in this section, I will argue that these methods have served a more uncertain purpose. In many cases, the level of specificity to the plans developed from these methods commit to certain assumptions about future states that run the risk of paving over uncertainties.

Often, argues Lee Clarke, the kinds of plans that organizations develop for uncertain and catastrophic possibilities do not actually serve to guide operations, but rather communicate confidence and accountability to the public and even organizations themselves. Clarke refers to such plans as "fantasy documents." Fantasy documents taken too seriously by an organization easily become unconscionable maps, not just symbolic but dangerous fantasies. And the way that security organizations have understood and practiced planning methods has contributed to a growth industry of unconscionable plans.

1. Scenario Planning

Scenario planning allows organizations to live in multiple futures rather than committing to and overinvesting in a single future.[275] As a method employed by Royal Dutch Shell in the 1960s scenario planning was a conscious departure from reliance purely on computational models to assess the likelihood of certain outcomes. Scenario planning asked organizations to engage in a creative conversation with possible futures, adapting and structuring their current posture based on multiple, different, plausible futures. This move towards considering plausible, not merely probable future conditions recognized the volatility of future conditions and served two purposes: challenging the

[275] Angela Wilkinson and Roland Kupers, "Living in the Futures," *Harvard Business Review* 91, no. 5 (May 2013): 118–27.

bias towards probability that existed in organizational culture at Royal Dutch Shell, and developing preparedness for more than one possible outcome.

In this, both the value and liability of scenario planning is visible. Scenario planning as an organizational exercise in self-knowledge and imagination prepares organizations for volatile futures. But scenario planning as a search for commonalities across different scenarios only reduces uncertainty for the scenarios considered. It does not reduce uncertainty for the scenario you were not able to consider.

Scenario planning for security applications owes its existence largely to the work of Herman Kahn, who pioneered the approach while at RAND Corporation in the 1940's and 1950s.[276] Given uncertainty in the actions of opponents (in Kahn's case, chiefly a Russian foe) scenarios offered a way to construct multiple plausible futures and consider them in detail. Rather than preparing for a single future, and committing too much to that possibility, scenarios were a structured way of hedging organizational bets against possibility. They also helped organizations to explore the possibilities of what might happen under different circumstances.

In this way, scenarios allowed American national security planners to understand the capabilities necessary to respond to multiple futures, and build a diverse set of capabilities rather than a single approach. It is a means of organizationally learning lessons. André Maginot is remembered for the strategic failure of the Maginot line: the meticulously planned and sophisticated fortifications meant to protect France from another German invasion in the wake of World War One. Scarred by the German invasion of the First World War, France invested heavily in hardening their border to protect against that possible future. And the Maginot line fortifications display other scars and lessons learned from the horrors of trench warfare—reflecting a civilized approach to fortifications that included retractable turrets. During world war two, Germany simply went around the fortifications and invaded through Belgium. Here scenarios appear as an imaginative form of risk. They are the exercise of imagination in considering plausible

[276] Herman Kahn, *On Escalation: Metaphors and Scenarios,* Hudson Institute Series on National Security and International Order (Piscataway, NJ: Transaction Publishers, 2009).

futures, considering and testing our responses to them. Like risk management, scenarios permit action in uncertainty.

Scenarios are equally subject to limitations. How many scenarios—how many possible futures—are sufficient? The national planning scenarios selected fifteen, but neglected EMPs and asteroids—plausible futures that suggested capabilities not covered in the other scenarios. "It is difficult," says Michael Barkun, "to create contingency plans for inconceivable contingencies."[277]

Faced with such apocalyptic possibility, it does seem important to plan for such eventualities. This presents a problem.

2. Capabilities-Based Planning

Scenario planning offers a means of living in multiple futures, but presented conceptual limits to uncertainty in the way that it bounded threats. Capabilities-based planning emerged as a means of decreasing the scope of uncertainty by developing a wider range of capabilities necessary to respond to a wider array of risks.[278]

Writing for the RAND Corporation, Paul Davis examined a new analytic architecture for defense planning that was applicable to a broad range of other planning applications.[279] His capabilities-based approach reversed the way that planners approached uncertainty by beginning with organizational self-awareness. The capabilities-based methodology was designed to reduce the margin of uncertainty by looking across multiple different scenarios or risks and developing exhaustive lists of the capabilities necessary to confront them. This allowed for a risk-based optimization of what capabilities organizations would need to develop, and in what quantity.

[277] Michael Barkun, "Defending Against the Apocalypse: The Limits of Homeland Security," *Policy Options* (September 2002).

[278] Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation* (Washington, DC: RAND National Defense Research Institute, 2005), 35.

[279] Ibid.

Capabilities-based and scenario planning are clearly not mutually exclusive. Both methods are designed for conditions of uncertainty, and both seek to reduce that uncertainty through the consideration of multiple potential outcomes. Where scenario planning is primarily an exercise in organizational imagination, capabilities-based planning is the accounting for scenarios through organizational capability development, and the search for commonality and structure to multiple plausible futures.

3. National Preparedness Planning

Since 2005, national preparedness planning conducted at the federal level has gradually shifted from scenario planning to capabilities-based planning.

HSPD-8 proposed a full-scale national approach to the management of crisis.[280] This took the form of scenario planning. The White House homeland Security Council served as the chair of an interagency committee that reviewed and developed 15 national planning scenarios thought to represent the spectrum of plausible national preparedness threats and hazards.[281] From these scenarios a universal task list was constructed, and these tasks were aggregated into greater capabilities.

The National, capabilities-based approach national preparedness planning has evolved from the comparative analysis of these "national planning scenarios" from which were extrapolated a set of "target capabilities" required across multiple scenarios, to an approach based on a Strategic National Risk assessment (SNRA).[282] From HSPD-8 to PPD-8 the shift was from scenario to risk, but the concept of capability development remained constant. The SNRA was designed as means to allow agencies to understand

[280] Executive directives have variable nomenclatures. Perhaps something can be read into the shift from specific homeland security Presidential directive to the more generic Presidential directives, or 1990's era national security presidential directives.

[281] Homeland Security Council, *National Planning Scenarios: Executive Summaries Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities* (Washington, DC: Homeland Security Council, April, 2005).

[282] Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation* (Washington, DC: DHS, December, 2011).

risks, and it was intended to impose greater rigor on the identification of necessary capabilities than the imagination of scenario planning.

Applied to national preparedness, the concept of scenario-based planning, or even deriving capabilities from scenarios suffers somewhat. The range of futures that must be considered is an expansive list. The National Planning Scenarios supposed fifteen plausible futures. The unconsidered possibilities of a catastrophic solar storm or climate disaster illustrate just how insufficient this number might be. The state of Ohio, for instance, considers thirty-five separate hazards in its State emergency operations plan.[283]

The National Preparedness System is the closest thing that the United States has to a comprehensive homeland security doctrine. The system itself is in its youth, born on paper in 2008 when PPD-8 replaced HSPD-8. However, the system has a much older lineage, dating at least back to the White House offices that initiated early civil defense programs and plans for rearmament in the wake of a Soviet attack.[284] Around the same time however, the large-scale flood control projects of the 1930s were taking shape under the Army Corps of engineers. The responsibility for managing flood and natural disasters remained spread out across multiple agencies not explicitly concerned with threats from attack. For this reason, the evolution of national preparedness has been a convergence of cultures: one focused on loss reduction and risk management, the other focused on threat management and civil defense. Along with these combined planning cultures came the imperative to address all hazards through national preparedness planning.

Both HSPD-8 and its successor PPD-8 claimed allegiance to an all hazards approach, meaning simply that every crisis contains common relationships and tasks, and the homeland security enterprise should focus on building up this generic capability to better respond to a broad range of threats and hazards. And they also both claim to be "capabilities-based." But their approaches are almost inverted.

[283] Ohio Emergency Management Agency, *Ohio Emergency Operations Plan, Base Plan* (July 2014), BP-5.

[284] John Fass Morton, *Next-Generation Homeland Security: Network Federalism and the Course to National Preparedness* (Annapolis, MD: Naval Institute Press, 2012), chapter 1.

Table 1. Comparing Planning Approaches HSPD-8 and PPD-8. After HSPD-8 and PPD-8.

HSPD-8	PPD-8
1. National Preparedness Vision	1. National Preparedness Goal
2. National Planning Scenarios	2. National Preparedness System
3. Universal Task List	3. Strategic National Risk Assessment (SNRA)
4. Target Capabilities List	4. National Planning Frameworks (across five mission areas)
	5. Federal Interagency Operational Plans (FIOPs)
	6. Incident Annexes

White House, *Homeland Security Presidential Directive (HSPD) 8, National Preparedness* (Washington, DC: White House, December 2003), and White House, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: March 30, 2011). The planning approaches contained in support of HSPD-8 and PPD-8 employ two different methods, but each consider a broad range of perils as the means to assess and calibrate capability development. Where HSPD-8 engendered reliance on scenarios, PPD-8 proposed a reliance on risks.

As concepts, HSPD-8 and PPD-8 are mirror twins. HSPD-8 arrives at capabilities from scenarios. PPD-8 arrives at incident annexes (akin to scenarios) from capabilities and concepts of interagency coordination. The SNRA, designed as a compendium and index of existing models of risks, informs both the FIOPs and the incident annexes. There are apparent affinities between the target capabilities of HSPD-8 and the core capabilities of PPD-8, but the process that undergirds them, and thus what they mean, is essentially inverted.

Though it is not acknowledged fully in the existing planning doctrine, PPD-8 changed national preparedness from a scenario-based approach for deriving national capabilities, to a risk-based one.

PPD-8 directed the development of a national preparedness goal that would, “appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them."[285] The National Preparedness Goal, published in 2011 contained the succinct summary statement that, "we define success as: A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[286] Risk, ideally, would then govern which capabilities the nation required. But facing catastrophic or highly uncertain dangers, using risk as a measure of capability development becomes somewhat illusory. If we can't predict the threat (probability) or the consequence (cost), it remains difficult to discern the best path for guiding capability decisions.

4. Threat Politics

Scenarios do not greatly reduce uncertainty. Dire, catastrophic scenarios contain another flaw: influence. Especially bad, uncertain, or fearful dangers are subject to public influence, social and organizational amplification, lobbying, and many forms of worry that is, it seems, disproportionate to the likelihood of the threat or hazard. This is the politics of threats.

The rarity, horror, and uncontrollability of a hazard impacts the way that Americans view that risk, and risk perception may even present its own risk. Given uncertainty, scenario planning as the basis for organizational action is particularly susceptible to "threat politics."

Returning to H.R 3410, security analysts may ask a forcing question: what conditions are necessary for a given hazard to warrant its own legislation?

There is ample reason to worry about EMPs. There is also ample reason to worry about catastrophic asteroid strikes, catastrophic climate change, and unbounded technological risks posed by nuclear power. Which of these require legislation? Which

[285] White House, *Homeland Security Presidential Directive 8: National Preparedness* (Washington, DC: December 17, 2003).

[286] Department of Homeland Security, *National Preparedness Goal, First Edition* (Washington, DC: DHS, September, 2011), 1.

require scenarios? Perhaps most importantly, how should homeland security professionals adjudicate scarce resources to address them? Our increased ability to predict and to do something about a wide range of threats often means an increased anxiety about what to do with limited resources. And conditions of uncertainty and volatility mean that hazards compete for attention.

The essential problem with scenarios, in this light, is that they can surrender risks to politics. The threat posed by a particular set of hazards, or a particular scenario is raised in prominence through advocacy, and one possibility can take resources from another equally likely (or equally uncertain) possibility. And this highlights the strange case of H.R 3410, a bill which sought to mandate a scenario onto the imaginations of planners.

But the overemphasis of single hazards and single scenarios has a damaging side effect. One of the central values of scenario planning was for organizations to engage in imagination. The scenario itself faded properly into the background, while the limits and strengths of the organization itself became the purpose and forefront of the exercise. Scenarios were mere tools for organizations to come to grips with how they might confront uncertainty. They were not designed as blunt instruments to rid the world of preparedness of the monster of uncertainty.

5. Not The Scenarios We're Looking For

Hilaire Belloc wrote *The Bad Child's Book of Beasts* in 1896 as a satire on the long tradition of moralistic children's tales.[287] Books like the 18th century *The History of Little Goody Two Shoes*, which followed the adventures of Margery Meanwell, were popular forms of using narrative and imagination to illustrate a principle or value.[288] Belloc's book pokes fun at this didactic literature. His book was written to bad (rude and wild) children, with the promise of making them, "unnaturally good" and the comic verse

[287] Hilaire Belloc, *The Bad Child's Book of Beasts* (Duckworth, 1896), introduction.

[288] Anonymous, *The History of Little Goody Two-Shoes: Otherwise Called, Mrs. Margery Two-Shoes* (London, UK: L.G. Challenger, 1766).

that follows tends to highlight the absurdities of human culture against a quiet nobility in the beasts themselves. Because it has the power to be compelling where mere facts may not succeed, narrative is often a vehicle for ideas.

How often are the scenarios that form the basis of homeland security plans simply didactic narratives? Have they ever attained Belloc's self-awareness? Inevitably, scenarios seem to reflect biases. While possibilistic thinking is necessary in the face of unbounded risk, scenario thinking can be particularly prone to threat-political interpretations. Here, scenarios can become cloying attempts at instruction, or mechanical process, blunting the value of a narrative with the plodding deliberation of a factory tour. The failure of imagination, if such a failure exists, is not corrected simply by imagining a sufficient number of scenarios. If scenarios are to be useful tools for imagination then they must encourage imagination as its own skill, not descend into guided tours through designed possibilities.

Robert Moore, vice president of Hewlett Packard's Global Security Services describes the boundless volatility of outcomes faced in a single year this way:

> Just touching on the headlines…We dealt with the fallout from civil unrest in Tunisia and Egypt at the beginning of the year, followed by the Christchurch earthquake in February, the Japan disaster and a state of emergency in Bahrain in March. In May, the capture of Osama bin Laden raised the possibility of retaliation. In June, there was an E-coli outbreak in Germany and unrest in Greece and Spain. In July, there were attacks in India and Norway followed by successive typhoons in the Philippines and flooding in Thailand.[289]

In situations where it is difficult to know what the future holds, scenario planning is supposed to allow the planner to consider multiple futures. This may improve preparedness through sheer numbers of potential outcomes considered, but it will not necessarily prepare organizations or individuals for the one scenario that was not considered but then occurs. The number of possible and probable and plausible futures outstrips our scenarios. If scenarios do not first serve to prepare planners and responders

[289] U.S. Resilience Project, *Priorities for America's Preparedness: Best Practices from the Private Sector, Resilience Roundtable* (Washington, DC: October 31, 2011).

to manage surprise and rupture, they are, it seems, little better than selecting one future and betting on it.

6. Scenarios Rightly Understood

As it has increasingly inherited a multiplicity of hazards, FEMA has adopted an all-hazards approach to planning, based largely on the capabilities-based approach. Capabilities-based planning, built on the assumptions of the SNRA has formed the backbone and baseline of a national approach to capabilities-based plans. However, the use of scenarios has also served as a powerful antidote to allowing national preparedness plans to descend into unconscionable territory. The source of this renovation of scenarios has come from Administrator Fugate's "Maximum of Maximums" approach to planning. Says Fugate:

> In emergency management we have only planned for what our capabilities can handle or only looked at what we can do to respond as government...But what we really need to be doing is planning for disasters that go beyond our capabilities. That's why we have to look beyond our government-centric approach and see what outside resources we can bring to the table.[290]

The maximum of maximum approach is effectively a "non-scenario." It is about coming to understand an organization at its limits, and learning to reach beyond them. It is not about the specific features of a given plausible future. The Response Federal Interagency Operational Plan developed as part of the National Preparedness System reflects this ethos.[291] As a document designed to guide the development of other plans, it orients the way that Federal resources are coordinated during disaster, and as such is, "[not] a contingency or implementation plan based on a specific threat or a scenario."[292]

[290] FEMA News Desk, "Release 101020: FEMA Administrator Craig Fugate Urges State Emergency Managers To Prepare For The Worst And Consider The Entire Community While Planning For Disaster, No.: HQ-10-203" (Washington, DC: October 20, 2010).

[291] Department of Homeland Security, *Response Federal Interagency Operational Plan* (Washington, DC: DHS, July 2014).

[292] Ibid., 3.

Scenarios are properly exercises in self-knowledge—increasing our understanding of our organizations and relationships. They acquaint us with our limitations and our strengths. As operational thought experiments, we should never mistake these maps for the territory, or the scenario for the future. And we base foundational plans on them at our peril. Rather, scenarios are simply tools for testing and expanding our ability to adapt to variable futures. In this sense, they are not really about the scenario at all.

This is why FEMA currently favors the "maximum of maximum" approach to planning and exercise design. The purpose of such an exercise is not simply to exercise a capability, but to understand means of responding when that capability is exhausted. It is a deliberate rupture of control, in order to map out limitations and discuss difficult tradeoffs and atypical options. In short: this kind of planning and exercising provides a model for the kinds of decisions that inevitably face emergency managers during crisis. In contrast, scenario-based planning efforts have large scale trickle down effects within the homeland security enterprise, notably in the way jurisdictions structure their grant requests. Scenarios can highlight a deficit in capability, but can equally be a mirage. Draft legislation such as H.R. 3410 remind practitioners that the debate over scenario-based strategy is not closed.

The next catastrophe or attack will be plausible. But only in hindsight. The value of scenarios is their ability to encourage organizations to exercise their imagination. The liability of scenarios is that organizations may be tempted to think that by considering scenarios, they have prepared for the next catastrophe.

C. MAPS OF NATIONAL UNIFORMITY

Upon an island hard to reach,
The East Beast sits upon his beach.
Upon the west beach sits the West Beast.
Each beach beast thinks he's the best beast.
Which beast is best?…Well, I thought at first
That the East was best and the West was worst.
Then I looked again from the west to the east
And I liked the beast on the east beach least.

—Theodor Seuss Geisel[293]

Maritime historian Marcus Rediker describes how eighteenth century naval ships were mobile organizations that also relied on tightly hierarchical labor arrangements. Walled off from the world by the ocean, organization onboard ships followed the strict hierarchies and stratifications of a closed society.[294] Maintaining the order necessary for the machinelike function of naval vessels reinforced a hierarchical model—from the captain, down through officers, noncommissioned officers and crew. Arguably, the exigencies of naval warfare required such strict command and control. Says Rediker, "the omnipotence of the elements and the fragility of human life marked the consciousness of every early-eighteenth century seaman."[295] Part of Rediker's insight, however, is to understand how thoroughly command and control aboard a ship depended on the isolation of the system. Command and control may have been necessary, but in order for it to exist, the conditions perhaps required a closed system. Sailing ships required isolation in order to preserve the conditions of command and control. The United States Military retains its own internal justice system, the Uniform Code of Military Justice, largely for the same reasons.[296] In order to preserve the internal orderliness of command and control structures necessary to provide for the common defense, a certain amount of overall separation of that system is necessary.

[293] Dr. Seuss, *Oh, Say Can You Say?* (New York, NY: Beginner Books, 1979), West Beast, East Beast

[294] Marcus Rediker, *Between the Devil and the Deep Blue Sea: Merchant Seamen, Pirates and the Anglo-American Maritime World, 1700-1750* (Cambridge, UK: Cambridge University Press, 1989), 1.

[295] Ibid., 2.

[296] Uniform Code of Military Justice, 10 U.S. Code Chapter 47.

The modern fire company is similar. Company captains, lieutenants, drivers and firefighters exist, train, deploy and operate in tightly controlled, hierarchical units. There are barriers to entry, and tightly structured means of advancing through experience, training and time in service. Fire trucks, when dispatched, illustrate mobile versions of that hierarchy. It is no surprise, then, that the lineage of ICS owes so much to fire service organizational models. If fire service organizations require command and control in order to function, they may also depend, as eighteenth century ships did, on conditions that permit command and control. ICS is such a system.

When hierarchical organizations came together during joint firefighting operations, lack of common organizational structure presented a command and control liability. The absence of a common organizational system prevented the integration of existing mechanisms for planning, resource allocation, and coordinated execution. But equally, restoring such a system required the invention of a common system. Preserving a common system, similar to Rediker's observation, required protecting it from the chaos of competing models.

The central idea that underlies NIMS and ICS is to approach the uncertainty and complexity of incidents with regularity and order—to impose order upon chaos. As an answer to the turbulence and ubiquity of unbounded risk, NIMS and ICS suppose that singularity, comprehensiveness, and the unification of all approaches under a common scheme are the answer to such risks. Standardization will permit seamless integration across disciplines and organizations. Uniformity will conquer chaos.

The stated purpose of NIMS is the provision of a, "consistent nationwide template" for the management of all incidents—from house fires to catastrophic hurricanes and terrorist attacks.[297] The scope of the NIMS guidance is national in the classical sense; it is meant to apply equally to government and the private sector, to federal, tribal, state, municipal governments and citizens. NIMS encompasses a national doctrine, an accepted practice that expresses a platonic concept of incident management.

[297] Federal Emergency Management Agency, *National Incident Management System* (Washington, DC: FEMA, December 2008), i.

It is a document that asserts a bold national truth claim: this is the way that America organizes to manage incidents.

The structure of the 2008 version of NIMS is prefigured by two “concepts and principles”: flexibility and standardization.[298] With somewhat circular reasoning, the 2008 NIMS doctrine explains that, “NIMS is flexible because the system components can be utilized to develop plans, processes, procedures, agreements, and roles for all types of incidents; it is applicable to any incident regardless of cause, size, location, or complexity.”[299] In other words, NIMS is flexible because all incidents require a standardized system. NIMS flexes by expansion or contraction of a universal form.

But at heart, these framing principles recognize that a standard system will find its application in many different situations. The purpose of a standardized NIMS then is to provide a common tongue for different organizations to work together.

NIMS proposes five components to its national system: Preparedness, Communications and Information Management, Resource Management, Command and Management, and Ongoing Management and Maintenance. The doctrine provides the concepts and principles that explain and guide each of these components. Not surprisingly, the concepts informing each of the five components stress uniformity, standardization, consistency etc. Command and management requires a, “fundamental form of management established in a standard format.”[300] Resource management requires consistency and a standard method for managing resources. This underlying purpose and intent for NIMS is to provide a *lingua franca* for incident management. Problematically, NIMS asserts that this language already fundamentally exists.

1. The Persistence of Scientific Management

In 1916, French Engineer Henri Fayol proposed an enduring idea that there are five essential functions to management: Planning, organizing, commanding, coordinating

[298] Ibid., 6. Which of these are a principle and which a concept is left to the reader’s imagination.

[299] Ibid.

[300] Ibid., 45.

and controlling.[301] Three years prior, one time president of the American society of mechanical engineers Frederick Winslow Taylor published *The Principles of Scientific Management*, in which he turned to engineering science as a tool to achieving national efficiency and maximum prosperity.[302] Greater efficiency in complicated manufacture and operations would, in Taylor's view, improve both the speed and quality of management systems. Scientific management was a means to optimize, get ahead and get better at it.

Bearing the mark of these influential schools of management, ICS was designed in the 1970s as a joint organizational model, "built to accomplish the five basic functions of any successful organization, Command, Planning, Operations, Logistics, and Finance."[303]

While NIMS does not provide much clarity around its four different kinds of management, the more important comparison with Fayol's characteristics is that both systems view organizations as machines. Like Taylor's model, ICS and NIMS are designed to produce ad hoc organizations that are able to rapidly combine and become efficiently engineered organizations.

The map, says Korzybski, is not all of the territory. The error and shortcoming of the NIMS component approach is that it creates an unconscionable map of organizational function.

2. The Appeal of Uniformity

Uniformity permits efficiency. The perceived value of the NIMS and ICS systems originated with the U.S. Forest Service Large Fire Organization model. This model was

[301] Henri Fayol, *General and Industrial Management* (London, UK: Pitman, 1949).

[302] Frederick Winslow Taylor, *The Principles of Scientific Management* (New York, NY: Harper, 1913), 10.

[303] Kimberly S Stambler and Joseph A Barbera, "Engineering the Incident Command and Multiagency Coordination Systems," *Journal of Homeland Security and Emergency Management* 8, no. 1. (January 23, 2011).

designed to bring disparate firefighting resources together and allow them to perform in a synchronized fashion.[304]

Wildfires exhibit complex behavior. They are susceptible to changing weather conditions and topography, their impacts variable depending on the impact area. Fighting fire requires the individual capabilities and organizational discipline of what would eventually become ICS because it permitted the expansion and contraction of the organization as the conditions of the fire changed and resources were brought in from multiple jurisdictions.

A uniform, national organizational model for incident management is appealing because it confronts incident complexity with organizational regularity; replacing unknowns with a known quantity. The responsibility of the ICS organization is to transform chaotic and complex incidents into complicated, but orderly objectives, dividing tasks across operational periods and systematically working to achieve objectives.[305] Not surprisingly, this has created a tendency for ICS to focus excessively on the intricacies of organizational models and approaches. The growth of ICS terminology and training is a reflection of the impulse to engineer incident response into an efficient organizational machine.

Complex incidents have a way of pushing back on orderly organizations. And it is a strange observable side effect of ICS organizations that they are uncomfortable with the inherent complexity of incidents. From its origins in Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE), ICS offered a regular set of tools for fighting the complexity and mutability of wildfire. But early minutes from the FIRESCOPE meetings are telling: “Dave Nelson. USFS, also gave a presentation on the

[304] Ibid.

[305] Cynthia Renaud, “The Missing Piece of NIMS: Teaching Incident Commanders How to Function in the Edge of Chaos,” *Homeland Security Affairs* 8, Article 8 (June 2012).

Incident Complexity Proposal. Radley stated he felt the presentation was overwhelming for the group."[306]

If, as some critics have suggested, ICS is designed to impose order on certain chaotic conditions in an incident, then the enduring complexity of an incident threatens to undermine one purpose of ICS.[307] Perhaps incident management is not the place for efficiency or the superimposition of coherence. The history of NIMS and ICS in particular suggests a discomfort on the part of responders with the endurance of uncertainty. And tools designed for efficiency may not be well suited to encouraging adaptation to complex risk.

The scientific management approach of NIMS and ICS tend to resist rather than acknowledge the inherent complexity of incidents. And when NIMS fails, homeland security organizations often learn the wrong lesson from such failure. Crises are inefficient problems. Decentralized, variable, uncertain threats that come with the problem of unbounded risk are not well suited to the centralized perception and decision model of command centric organizations.

3. Fighting Federalism

Decentralized risks have only accelerated the quest for uniformity. The way that unbounded risks cross-political boundaries and artificial sectors and geographic limits, combined with our precautionary approach in the wake of 9/11 has led homeland security to chafe against federalism in the name of security.

Reduced to a national preparedness axiom, the principle of federalism in American government is a reminder that mayors do not work for governors do not work for the President. And citizens work for none of these. American government was designed with a high degree of intentional inefficiency. The principle of enumerated and

[306] FIRESCOPE, "Operations Team Meeting" (meeting minutes, Los Angeles County Fire Department, Lac Camp #2, March 30, 1987).

[307] Dick A. Buck, Joseph E. Trainor, and Benigno E. Aguirre, "A critical evaluation of the incident command system and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006).

balanced powers originates with an idea about the nature of man—that he was endowed by his creator with certain inalienable rights. A government with enough power to preserve those rights might be able to abridge them, and so needed to have built in limitations and controls. The design of the Constitution was a decentralized national approach to government that recognized state and local sovereignties, as well as distinct federal government authority to exert certain limited national powers. Further complicating matters, the American system of separating powers among executive, legislative and judicial branches of government ensured that the process of editing and refining government powers was arduous.

This is the operating environment for incident management.

In the context of national preparedness, this presents stark difficulties. In disaster, the efficiency of NIMS and ICS runs into a carefully designed network of government that thwarts the establishment of a uniform, centrally controlled machine organization with control over intentions, resources and operations. Prevented from imposing a system of command and control that draws a red line from the President down to the citizen, NIMS pursues a model of "unified command."

Unified Command, as expressed in the NIMS doctrine is a concept that, when the impact and operations of incidents span multiple jurisdictions political boundaries, "allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability."[308] And yet this voluntary concept of jurisdictional cooperation contains a caveat. As a footnote to the concept of, "chain of command," NIMS acknowledges that:

> Concepts of 'command' and 'unity of command' have distinct legal meanings for military forces and operations. For military forces, command runs from the President to the Secretary of Defense to the Commander of the combatant command to the commander of the forces. The 'Unified

[308] Federal Emergency Management Agency, *National Incident Management System* (Washington, DC: FEMA, December 2008), 49.

> Command' concept utilized by civil authorities is distinct from the military chain of command.[309]

As a doctrinal "get out of jail free" card this quotation highlights an oddity with the idea of unified command, admitting to the way that large incidents chafe against the complexity of federalism. Unified command appears to be a consensual myth: voluntary and cancelable.

The military, as exemplified in the quotation, has discrete legal authorities and limitations that make it clear that it does not simply integrate into a unified command structure. More accurately, the footnote would acknowledge that civil authorities likewise do not divest their chains of command. They remain differently, but equally as independent as the military chains of command during large-scale incidents.

Incidents such as the Deepwater Horizon oil spill have highlighted the way that doctrines can collide against federalism. The "Shared Power" doctrine of unified command also collides with other federal doctrine that supposes a greater degree of control at the federal level—resulting in what has been called "doctrinal confusion."[310] The Hurricane Sandy FEMA After Action Report highlighted similar uncertainties about how to establish and cultivate a "unified coordination group," which doctrinally serves as the principal organizing construct for working across jurisdictional entities.[311]

The observation may be simple enough to seem absurd, but the chief reason that national incident management has not achieved uniformity after a decade of sustained national effort is likely the reality that such uniformity does not exist. The shape and responsibility of governments across the United States were not engineered from a central planning department, but grew up around the needs and shapes of the communities within those states. The idea of NIMS, imposed through grant requirement, is designed to, in the

[309] Ibid., 48.

[310] Thomas A. Birkland and Sarah E. DeYoung. "Emergency Response, Doctrinal Confusion, and Federalism in the Deepwater Horizon Oil Spill." *Publius: The Journal of Federalism* 41, no. 3. July 1, 2011: 471–93.

[311] FEMA, *Hurricane Sandy FEMA After Action Report* (Washington, DC: July 1, 2013), 12.

realm of incident management, begin to move towards a common, engineered approach. But the entities involved in emergency management are not restricted to incident management organizations, and operate on a day-to-day basis within the shape and function of their own sphere.

Considering "NIMS implementation behaviour" Jessica Jensen observed that states and localities adopting NIMS as required for grant funding, are heavily modifying it.[312] NIMS doctrine as written allows for a certain degree of local adaptation. However, the forms of adaptation taken at the implementation level nationwide are significant enough that Jensen argues it may undermine the use of NIMS as the basis for national incident management. Perhaps more starkly than Jensen concludes, the extreme variability of approaches across jurisdictions may undermine the usefulness of any national incident management model.

National uniformity may be an unconscionable map. It may also be fundamentally unachievable. Perhaps worse, were NIMS to succeed in producing a nationally uniform scheme of operations, such efficiency might in fact present security liabilities.

4. The Liability of Uniformity

The prevailing narrative of crisis and catastrophe response is not the disciplined deployment and coordination of known quantities, but rather the incorporation of unknown capabilities, and the rapid adaptation of uncommon partners to new circumstances.

When NIMS fails, the assumption is often that this failure has to do with lack of operational discipline or incomplete training and awareness. But the uniformity of NIMS can also degrade organizational adaptability. FEMA doctrine provides for three models of organization post disaster: Geographic, functional, and a hybrid approach.[313] This is based in part on the persistence of principles of scientific management—tools for

[312] Jessica Jensen, "The Current NIMS Implementation Behavior of United States Counties," *Journal of Homeland Security and Emergency Management* 8, no. 1. (January 2, 2011).

[313] FEMA, *Hurricane Sandy FEMA After Action Report* (Washington, DC: July 1, 2013), 12.

maximizing the efficiency of an organization. Such arrangements are designed for efficiency, not maneuverability. When a NIMS organization has to change and adapt to evolving impacts and requirements, it confronts similar challenges to a factory owner deciding to reconfigure or re-tool an assembly line.

Implementing incident management structures was presented as an area for improvement in the Hurricane Sandy FEMA After Action Report. Responding to Hurricane Sandy required FEMA to address an overarching operational challenge—coordinating a federal response across multiple states each with differing political boundaries, geographic features, infrastructure sectors, impacts and populations. The approach taken was designed to, “facilitate centralized program decision-making, while ensuring appropriate geographic coverage.”[314]

The intent of FEMA’s selection of an operational model, as with NIMS and ICS approaches in general, was to centralize decision making as a means of ensuring efficiency, productivity, and meeting the needs of those impacted. As the relief effort progressed, some operational components devolved responsibilities in some areas increasingly to geographic divisions, while others resisted decentralization of authority. To complicate matters, as multiple federal agencies addressed impacts:

> Sandy response efforts revealed that several [emergency support function] coordinating agencies have adopted a more department centric approach to response operations, rather than the integrated functional approach prescribed by the [national response framework]. In these instances, ESF coordinating agencies did not fully draw upon the capabilities of supporting departments and agencies.[315]

This observation suggests that individual departments and agencies failed to integrate properly into the coordinated incident management structure. They did not effectively work within the efficient NIMS machine.

[314] Ibid.

[315] Ibid.

Sandy, however, may offer a similar lesson to Deepwater Horizon and other complex disasters. On the one hand, responding agencies and departments failed to integrate. On the other hand, organizational models failed to adapt to the reality of impacts and requirements. This may demonstrate more than a breakdown in organizational discipline, though that may well be true, emphasizing a limitation to the use of organizational models that require such disciplined integration in the first place.

It is the perennial duty of after action reports to prescribe more training. If individuals and groups responding to Sandy had been more expert in the organizational imperatives of the system, then perhaps they would have been able to integrate more readily in a seamless fashion.

Conversely, engineered organizational models of incident management may need to more readily acknowledge the complexity of disaster impacts and the corresponding complexity of agencies and capabilities. ICS and NIMS are orderly. But if incident command and management is not sufficient to get all the players to align and integrate, the alternative may not be chaos. Perhaps there is a better way.

Post disaster organizational structures that respond to and reflect the operational environment would require a radical rethinking of the engineered organization. Organizational structures would have to allow national teams to cross political boundaries when necessary, to address geographical concerns as needed, and to address cross cutting subject specific issues as needed. This would mean admitting to the multiple overlapping nature of authorities and capabilities at play in an operation, the border crisscrossing impacts to infrastructure systems, and the need for a form of community engagement that takes the shape of a community, rather than superimposing an incident structure over the top of it.

This does not mean institutionalizing chaos, but rather means acknowledging the truth of complexity. ICS contends that common internal organization is necessary to confront complexity and chaos. NIMS contends that this is necessary nationally.

5. Two Competing Doctrines

Emergency management doctrine promotes the concept that everyone is an emergency manager, and the "whole community" of the nation is central to disaster response. As expressed by FEMA administrator Craig Fugate, "Individuals and communities are key assets, not liabilities. They offer specialized knowledge and skills, provide neighbor-to-neighbor assistance, and allow emergency responders to focus their resources where they are most needed."[316] For the future of NIMS, and the impulse to nationalize it as a system, this presents a troubling dual doctrine. If everyone in the nation is a part of crisis response, then everyone must be trained on NIMS in order to fully participate in response.

We must first ask whether such a thing is possible. We must then wonder whether it is desirable. Each case seems doubtful. Just as the risk society thesis argues the unbounded complexities of risk create a gulf between individuals institutions responsible for managing those risks, the exponential complexity of incident management structures, rules and training act as impediments to the doctrine of "whole community" emergency management. This is not to argue that incident management is simple, and requires a simpler discipline. Quite the opposite. It is to argue that incidents are inherently complex, and defy any single system. And despite its abstruse rules for functional structure and hierarchy, the concept of incident command in fact proposes to simplify the solutions to incident complexity. This presents a barrier to innovation during operations.

6. NIMS Unbound

Writing in 2013, Cynthia Renaud argued that the structures of incident command outlined in the National Incident Management System are incomplete.[317] The relevance and usefulness of command and control architectures, especially the ICS that is part of

[316] Hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C. Release Date: March 17, 2011 (Testimony of Craig Fugate, Administrator, Federal Emergency Management Agency).

[317] Cynthia Renaud, "The Missing Piece of NIMS: Teaching Incident Commanders How to Function in the Edge of Chaos," *Homeland Security Affairs* 8, Article 8 (June 2012).

NIMS may, according to Renaud, have a lower bound. In the initial moments following incidents, or at a highly localized level, the prefabrication of the ICS system may not lend itself well to the undiscovered and ill-defined parameters of an incident. In this space, incident commanders must cultivate something Renaud identifies as an almost intangible quality of sense making and leadership.

The lower bound of NIMS and ICS is a question of sensing and decision-making. The efficient, scientific organization of NIMS and ICS does not describe the unstructured, often improvisational efforts that characterize much crisis decision-making.

If NIMS and ICS are organizational systems subject to a lower bound, they may also have an upper bound. In unbounded risk, incidents can achieve a scope, scale or complexity that diminishes the usefulness of command and control structures.

7. The Myth of the Typed Resource

It might have been the beginning of a joke, were it not a serious problem: how many utility trucks can you fit on a C-5? Prior to Hurricane Sandy, the Defense Logistics Agency, the Department of Energy, FEMA and private sector utility companies had not developed load plans for airlifting utility trucks into disaster areas to effect power restoration. And yet, in 2012, that became a central logistical problem to solve, as the DOD helped move Southern California Edison Utility Company equipment and personnel to support the relief effort.[318] Due to the change in air pressure during flight, utility trucks need to have the air let out of tires not designed for such pressures. This was not written in any operational plan prior to the incident.

In response to disaster, professionals solve such problems as a matter of course. Adapting to these uncertainties is arguably the central prevailing narrative of large-scale emergency management. But airlifting unfamiliar equipment encourages another impulse as well; it seems to support the case for “typed” resources. For almost a decade, FEMA has pursued the construction of a catalogue of national resource type definitions—

[318] Jim Garamone, “DOD Launches ‘Airlift Event’ to Support Sandy Relief,” *DoD News*, Washington, November 1, 2012.

covering everything from people to equipment, from advanced emergency medical technicians to Wheel Dozers. The hope for the Resource Typing Library Tool (RTLT) is a complete compendium of disaster resources, with nationally standardized definitions.[319] But there is no current resource type for utility trucks.

The concept behind nationally typing resources makes sense. If the qualifications, training, shape, size, weight and other pertinent dimensions of every resource are known and catalogued as a national standard, then developing, maintaining, deploying and managing those resources becomes a scientific matter of national resource awareness. This may be unachievable for many resources, but it also may represent the ultimate unconscionable map. The list will never be exhaustive, the nature of resources will change more rapidly than the list and the plans built from an incomplete and perpetually out of date list will be incomplete and perpetually out of date. Such plans will, invariably, forget that they are maps.

The development of national resource types has been plagued with difficulties. The list of typed resources is incomplete, and out of date. There is no national standard adhered to for virtually any typed team or asset. And the next necessary resource that will become needful during catastrophe is probably not even on any list. There doesn’t seem to be agreement, nationally, one what certain resources consist of. This raises the possibility that resource types may actually differ from state to state, or from discipline to discipline. Why is it so difficult to type resources?

The limitations of resource typing may be the same limitations of scenario and capability-based planning. While scenario planning is useful as a means of exercising organizational imagination it is limited as a tool for preparing for different potential outcomes. Resource typing suffers a similar fate. In such cases, Lewis Carroll whimsically argued, the country may serve better as its own map, without the imposition of an unconscionable one.

[319] Federal Emergency Management Agency, “Resource Typing Library Tool (RTLT)-v1.3.0.” Accessed August 1, 2015. https://rtlt.preptoolkit.org/Public.

D. PORTOLAN CHARTS: COMMAND AND CONTROL

> *Any system comprising multiple, interacting elements, from societies to sports teams to any living organism, needs some form of command and control. Simply put, command and control in some form or another is essential to survival and success in any competitive or cooperative enterprise. Command and control is a fundamental requirement for life and growth, survival, and success for any system.*
>
> —Marine Corps Doctrine[320]

> *Thus, seated, [King Canute] shouted to the flowing sea, 'Thou, too, art subject to my command, as the land on which I am seated is mine; and no one has ever resisted my commands with impunity. I command you, then, not to flow over my land, nor presume to wet the feet and the robe of your lord.' The tide, however, continuing to rise as usual, dashed over his feet and legs without respect to his royal person.*
>
> —Henry of Huntingdon[321]

Martin Waldseemüller's 1507 world map depicts two sea monsters that signal the dangers of the unknown ocean. His 1516 *Carta Marina*, in contrast, depicts king Manuel of Portugal astride a sea monster, indicating political and technical mastery of oceans previously seen as unknown and dangerous.[322] The dynamic illustrated is that with knowledge comes control.

This section addresses the question of whether command and control are compatible with unbounded risk. Unbounded risk places a particular burden and challenge to the concept of command and control. National preparedness doctrine, by contrast, places great emphasis on command and control. This presents a problem.

The emphasis that Marine Corps doctrine places on command and control is frank and universal. Command and control in the Marine understanding is not a military

[320] United States Marine Corps. *Command and Control (Marine Corps Doctrinal Publication 6)* (U.S. Marine Corps, 1996), 36. While written in 1996, this doctrine is current as of 2015.

[321] Henry of Huntingdon, *The Chronicle of Henry of Huntingdon, Comprising the history of England, from the invasion of Julius Cæsar to the accession of Henry II, Also, The acts of Stephen, king of England and duke of Normandy*, edited and translated by Thomas Forester (London, UK: H. G. Bohn, 1853), 199.

[322] Chet Van Duzer, *Sea Monsters on Medieval and Renaissance Maps*, 76.

doctrine but a fundamental statement about the world. With this understanding, command and control is to be examined, fostered, cultivated and optimized for the functioning of organizations and endeavors. Elsewhere, military command and control has complementary and competing definitions:

> Command and control [is] the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.[323]
>
> The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.[324]

Each definition is tailored to its purpose. The DOD definition, built for the context of joint or interagency operations, is careful to include the concepts of designated authority and assigned responsibility. The Marine Corps definition is more essentially philosophical. It is about command, control, and the commander. But both share a common idea. In situations that require action, there is a commander, and appropriate action. And the commander's obligation is to recognize and ensure that action.

It is an appealing concept. Faced with ambiguity, external threat or difficulty, the commander must exercise discipline and initiative to accomplish a group objective. The commander is the central figure in this story—the means for getting something done.

It is perhaps not surprising then that NIMS and ICS place such emphasis on command and control. It is largely accepted in incident management doctrine that command and control is necessary. It is "established" post-incident, and incidents and disasters are often viewed as events that create a rupture with the existing command and control, requiring ICS structures in order to re-assert command and control on situations. In incidents then, society turns to incident management organizations as experts in asserting this fundamental concept back onto chaos and destruction. In this sense,

[323] United States Marine Corps, *Command and Control (Marine Corps Doctrinal Publication 6)* (U.S. Marine Corps, 1996).

[324] Department of Defense, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010* (As Amended Through 15 January 2015), 40.

command and control are more than simply schemes to organize response organizations. It is a fact of society to be cultivated and maintained.

In early December, 2014, the National Infragard Electromagnetic Pulse Special Interest Group convened a workshop and tabletop exercise to consider high impact threats to the electric grid. The group considered three scenarios, developed by a panel of experts in their respective fields.

Four weeks into a blackout, says the scenario, “law enforcement has been replaced by Marshall [sic] Law” along with the “first signs of breakdown of social order.”[325] Sooner than that, “barter will predominate for commerce,” meanwhile, “gangs roam the streets,” looting. The impacts are far worse in cities where, says the scenario, individuals are less self-reliant. The disaster overwhelms, despite the heroic efforts of the military to restore command and control, and protect fuel convoys from the ravages of gangs. One of the central questions of the scenario was whether the participant’s jurisdiction has a, “command and control structure that can deal with such a catastrophe.”

Despite the emphasis on command and control, it may not be a model well suited to unbounded risk.

Unified command is, as we have seen, an organizational half-truth. Footnote and law exempt the military from it, and civil authorities participate in it only as a consensual arrangement, cancelable when the needs of unified coordination groups no longer speak to the needs of a municipality or infrastructure sector. As in the case of the Lac- Mégantic rail accident, the entities responsible for managing such risks cannot have a common command and control structure.

National incident management doctrine refers to, “establishing command and control.”[326] Here we encounter the truth claims, the philosophy of command and control. The rupture caused by incidents requires group action, and disparate parts must work

[325] National Infragard EMP Special Interest Group, “High Impact Threats to the Electrical Grid: Workshop and Tabletop Exercise,” 2015, 37.

[326] Federal Emergency Management Agency, *National Incident Management System* (Washington, DC: FEMA, December 2008), 28.

together for a common end. As such, they require commanders to establish command and control. Returning to the Marine Corps definition, disasters cry out for a commander with the means to recognize and see to appropriate actions.

But in domestic crisis, commanders often do not have command or control. Recognizing that individuals and organizations outside of the official and designated response personnel may play a critical role in weird or uncommon dangers means one of two things. Every citizen and group must have a working knowledge of the common operational system in order to respond effectively, or a national incident management system requires some limits. As discussed, the idea that every American citizen will be, or should be trained on NIMS is an uncertain concept.

It should not surprise us to discover that organizations designed to superimpose order upon chaos are not well adapted to managing enduring uncertainty. While command and control is successful and essential doctrine within the sphere of military missions and coordinating disciplined resources assigned to a centralized command structures, it is unsuitable as a foundational philosophy for national incident management.

Isaac Newton's second law of motion stated that, "the alteration of motion is ever proportional to the motive force impressed; and is made in the direction of the right line in which that force is impressed."[327] Newtonian physics, in order to establish such laws, presupposes a closed system, in which the conditions within the system are static and not subject to the influence of "outside forces." Domestic crisis and disaster management are inherently open systems—impacting multiple jurisdictions and drawing resources from local, state, and Federal organizations, as well as national organizations and companies. For this reason, incident command and control is vital in a limited application, but inappropriate as a national system for incident management.

[327] Sir Isaac Newton, *The Mathematical Principles of Natural Philosophy*, translated into English by Andrew Motte (London, UK: H.D. Symonds, 1803).

E. CONCLUSION

Homeland security often implicitly promises perfection. This has meant that security organizations are highly susceptible to dramatic redefinition in the face of catastrophe. The thesis here is that we need an explicit doctrine of uncertainty.

The problem goes beyond structural deficiencies in NIMS, or problems with the application of ICS, although the deficiencies are great, and the limitations in application are serious. As I have assessed in this chapter, National Preparedness may be better served by the abolition of NIMS along with the aspiration to national uniformity. What is wanting is not a common tongue, but a common skill: adaptability. In the next and final chapter I will argue that *national adaptability* is more desirable than *national uniformity*. This means a variegated landscape, and it means a different set of skills for responders.

Our response to unbounded risk in much of our doctrine and organizational arrangements is to pretend that we can manage and control more than we are able. Command and control models for crisis management hinder rather than support adaptive organizations. We pretend with catastrophic planning that still catalogues actions and execution schedules. And we presume to unattainable knowledge with bulk data collection and boundless precaution (guns gates and guards). Such responses are reactive to enduring uncertainty—uncertainty that remains despite risk assessment—so our security agencies find themselves doing everything to avoid anything. However, it is not entirely possible to know how successful such precaution has been, and our current approach lacks any limiting principle. Homeland security is not able to say how much of what is enough.

FEMA advises that emergency kits equip individuals and families for at least 72 hours.[328] There is little literature to suggest an origin for this three day minimum, and less to bear out in practice its utility. Naturally, this thesis is not arguing for a lower time frame of preparedness. But it is worth considering that this 72-hour bar of preparedness is not based on either the character of hazards or the character of governmental response.

[328] Federal Emergency Management Agency. “Build a Kit.” Last Accessed August 1, 2015. http://www.ready.gov/build-a-kit.

There is no average disruption of 72 hours, and no average catastrophic response or rescue time of 72 hours. It is, in short, largely arbitrary. It is a good idea, but no better than 100 or 200 hours of planned survival. It is a time frame invoked, rather than advised. The purpose of challenging this accepted number is not to discredit preparedness, but to highlight a tendency that security and planning practices have towards arbitrariness and presumptions of control. For this number surely communicates more than simply a lower bound of disaster. You will find the 72-hour number not just in guidance for individual readiness but also in guidance for incident responders. 72 hours is a benchmark for establishing incident command.[329] 72 hours is a time frame for initial planning assumptions, and the transition of operational control to field personnel.[330] It is a figure often invoked for these purposes, and it openly frames an important question. What are we to make of catastrophe that extends beyond this 72 hour mark?

National uniformity in a lot of the NIMS effort is paving over inherent adaptability set up by federalism. Fortunately, in many cases, it is skills already in development, constrained by aspirations to uniformity. Homeland security needs to unleash such adaptability.

[329] FEMA, *Hurricane Sandy FEMA After Action Report* (Washington DC: July 1, 2013), 14.

[330] Ibid.

IV. UNSEEN DOCTRINE

> *Fish don't try to turn sharks into vegetarians. Living immersed in a world of constant risk forces the fish to develop multiple ways to live with risk, rather than trying to eliminate it.*
>
> —Raphael Sagarin[331]

> *Great and terrible flesh-eating beasts have always shared landscape with humans. They were part of the ecological matrix within which Homo sapiens evolved. They were part of the psychological context in which our sense of identity as a species arose. They were part of the spiritual systems that we invented for coping. The teeth of big predators, their claws, their ferocity and their hunger, were grim realities that could be eluded but not forgotten. Every once in a while a monstrous carnivore emerged like doom from a forest or a river to kill someone and feed on the body. It was a familiar sort of disaster–like auto fatalities today–that must have seemed freshly, shockingly gruesome each time, despite the familiarity. And it conveyed a certain message. Among the earliest forms of human self-awareness was awareness of being meat.*
>
> —David Quammen[332]

Sledding on Capitol Hill has been banned since the attacks of 9/11. In 2015, following a snowstorm in the Washington, DC area, citizens banded together in an act of civil disobedience and defied the capitol traffic regulations prohibiting such sledding. The chairman of the Capitol Police board reiterated a ban on sledding, "for security reasons," but legislators listened to and responded to the organized "sled-ins" that resulted. Bearing signs of, "sled free or die," citizens, literally, took the hill. In May of 2015, a legislative branch funding bill instructed Capitol Police specifically to, "forebear enforcement,"

[331] Rafe Sagarin, *Learning From the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease* (New York, NY: Basic Books, 2012), 21.

[332] David Quammen, *Monster of God: The Man-Eating Predator in the Jungles of History and the Mind* (New York, NY: W.W. Norton & Company, 2004).

when they encountered sledding.[333] This offers a lesson in responsive government. It illustrates further that it is possible to roll back securitization, and temper precaution.

It is a humorous, charming episode. But this belies a more serious point about security. Citizens on Capitol Hill prefer sledding to the margin of safety provided by the sledding ban. This means they prefer the danger. This is defiant, contrary to the precautionary principle. When facing unbounded risk, it may also be good policy.

Early in this thesis, I posed a rhetorical question that remains unanswered: Is catastrophe just chance we could not tame? Are ambiguous threats the leftover uncertainty that security organizations were unable to render into risk? Part of the answer is that America must discover the best way to live with danger. Homeland security cannot provide perfect security. And yet, the broad emphasis on precautionary measures, planning paradigms, nationally uniform incident management structures and command and control philosophies implicitly pursues and promises a greater degree of control than is possible.

Sledding on Capitol Hill present no greater or lesser danger of terrorism in 2015 than it did in 2002. But in the uncertainty of unbounded risk, values matter more than methods. For greater or lesser security, the tradition of sledding can trump security concerns.

If homeland security is to inhabit especially dangerous and uncertain waters, this must mean new doctrine. In this chapter, I will consider what this task requires of homeland security professionals and evaluate available tools for confronting the enduring uncertainty of the risks they face.

Thus, far, I have presented a bleak assessment. Risks are extending beyond the ability to know or control them, and security professionals venture to secure a wilderness equipped with a series of deeply institutionalized myths. Organizations pretend to control, and attempt to impose order on increasingly non-responsive risks. Our

[333] Kelsey Snell, “House Votes to Bring Sledding back to Capitol Hill,” *The Washington Post*, May 19, 2015.

philosophies of command and control may even be making us less safe as they fail to acknowledge the volatility of risk or the chaotic dimensions of response. And the dominant mode of precaution may be strangling our ability to provide meaningful security measures. Homeland security arrangements are often ill suited to the reality of danger and catastrophe.

And yet, if homeland security is to earnestly turn its attention to the problem of insecurity and uncertainty, there is significant literature and thinking which can renovate our practices and our doctrines. Faced with unbounded risks, the concept of national preparedness may be able to reform itself around a new set of theory and practice.

There is great danger and great utility in believing our own fantasies. Trusting in the unconscionable maps made for cataclysms, organizations may become too comfortable, too complacent and wedded to conjecture. However, they might equally make the opposite mistake, allowing us to become the madman described in A Midsummer Night's Dream—who sees more devils than hell can hold.[334] To understand unbounded risks aright requires a tempered catastrophism. Security organizations must admit to risks they cannot control and balance precaution against exploration and readiness for surprise.

A. REASONABLE SECURITY

Joint Intelligence Briefing products developed through the Office of the Director of National Intelligence often remind the reader that many suspicious activities are constitutionally protected behaviors. Another way of expressing this reality is that democratic society is not designed to be unreasonably safe.

John Witherspoon, long time president of what would become Princeton University, signer of the Declaration of Independence, and teacher to many of the American founding fathers considered theoretically what it meant for a nation to provide

[334] Shakespeare, William, *A Midsummer Night's Dream* (Philadelphia, US: J.B Lippincott and Co., 1895).

"reasonable security." Says Witherspoon, "perhaps it may be asked what is reasonable security against future injury."[335]

Witherspoon recognized that absolute security might be totalitarian and was impossible anyway. It is perhaps a considerable irony that 18th century governmental theory should display such cold realism, while current national preparedness doctrine reflects an almost utopian confidence:

> A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.[336]

It may be semantic scolding to observe that a nation in possession of the capabilities to prevent all threats and hazards need not worry about responding to them. But it may also indicate that homeland security has lost the ability to understand itself in terms of the provision of reasonable security. Homeland security may be in pursuit of unreasonable security.

In Federalist Paper No. 24, Alexander Hamilton warned that, "Though a wide ocean separates the United States from Europe, yet there are various considerations that warn us against an excess of confidence or security."[337] Considering the provision for the common defense, Hamilton argued that an excess of confidence or security must be tempered by realistic assessment of possible threats—this, in Hamilton's view, justified the provision for a standing military. But this not an unlimited principle. Just as an excessive confidence in safety must be tempered by provision for security, a nation can excessively pursue security. The growth of unbounded risk, as we have seen, makes it difficult to know what reasonable or excessive security looks like. For this reason, a

[335] John Witherspoon, *The Works of John Witherspoon, D.D* (Edinbourgh, SCT: Ogle and Aikman, J. Pillans, J. Ritchie, J. Turnbull, 1805), 111.

[336] Department of Homeland Security, *National Preparedness Goal, First Edition* (Washington, DC: DHS, September, 2011), 1.

[337] Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers* (Mineola, NY: Dover Publications, 2014), 111.

doctrine of reasonable security must begin with the acknowledgement that we accept and live with a certain amount of danger.

Here the concept of risk is reborn as a proposition of value. Risks are not things that happen to us, risks are instead taken. It may be counted a small thing, but sledding on Capitol Hill represents an important step in America taking and accepting risks. Reasonable security means living bravely.

There is potentially deep absurdity to the precautionary principle. For one, it has no evident limiting principle. To be cautious about everything requires equal caution about taking action against anything, lest intervention bring with it unseen risks. If something is possible, must we do and expend everything against it? How do we address competing claims? Does precaution require us to simply surrender to our fears of what is possible? How do we choose between apocalypses, and which possible danger deserves our attention?

Much of the effort to respond to volatile and devastating risks has exhibited itself as an effort to impose control over the uncontrollable. We can see the outworking of this thought in our national counterterrorism strategies, and in some of the progressive steps taken by European governments in addressing the catastrophic possibilities of climate change. The principle has an immediate appeal. If we cannot quite discern how likely something is to happen, and cannot cleanly project the scope of its impact, then it makes sense to pursue some action rather than no action. We are a precautionary people.

Cass Sunstein's "anti-catastrophe" principle provides an organizing doctrine for confronting and tempering excessive precaution. Assessing competing worst-case scenarios may serve as a means to prevent neglect of dire possibilities such as catastrophic climate change, and politicization of one hazard over another. The anti-catastrophe principle does not promise perfect security, but it provides a disciplined approach to thinking about our plans and atlases that need not plan for every eventuality, but identify and organize against unacceptable futures.

Unbounded risk demands new doctrine. Crisis management expert Patrick Lagadec argues, “it would be a historic blunder to prepare the new generation of leaders for the risks and crises of the last century.”[338] As risks and crises change, doctrine needs to evolve and adapt.

B. THE DOCTRINE OF MULTIVALENCE

> multivalent (adj.)
> 1874, from *multi-* + *-valent*, from Latin *valentem*, present participle of *valere* “be worth” (see *valiant*).
>
> —Online Etymology Dictionary

> *A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly. Specialization is for insects.*
>
> —Robert Anson Heinlein[339]

A doctrine of unbounded risk precludes the imposition of a national incident management structure. It precludes the imposition of excessive control mechanisms, and makes a mockery of overly scripted plans for uncertain futures. Security doctrine for unbounded risk must instead be multivalent. Multivalence means possessing and incorporating the competing values of different systems. Military command and control must live symbiotically with unstructured community organizations. Decentralized volunteer groups must coexist productively with teams of forensic engineers.

NIMS claims to be this system, eliminating differences in approach by creating a common national one. But if the central narrative of catastrophe, crisis, and threat is not the efficient deployment of known quantities, but the adaptive capacity of previously unknown partners, then NIMS will always be out of reach. Security doctrine must

[338] Patrick Lagadec, “Leadership in Terra Incognita – Mapping the Way for Senior Executives,” *Crisis Response Journal* 6, no. 3, 2010.

[339] Robert Heinlein, *Time Enough for Love* (New York, NY: Penguin, 1987).

conform to a new task. Here I propose four characteristics of multivalence for security doctrine.

- Adaptability: The ability to sense and quickly respond to changes in the risk environment.
- Pathfinding: The capacity for confident exploration of uncertainty.
- Mapmaking: The ability to produce maps for uncharted landscapes.
- Reconciling: The disciplined organizational humility regarding of the limits of safety.

1. Adaptability

> *We are a wild species, as Darwin pointed out. Nobody ever tamed or domesticated or scientifically bred us. But for at least three millennia we have been engaged in a cumulative and ambitious race to modify and gain control of our environment, and in the process we have come close to domesticating ourselves.*
>
> —Wallace Stegner[340]

Adaptability is a buzzword—a concept more often invoked than understood. We're often told that our organizations need to acquire and develop it. Why? It is easy for disciplined and experienced responders to view the idea of adaptation as undisciplined, chaotic, irregular, or more often just amateur. In this view, adaptability looks like free jazz—its rebelliousness is its purpose. Convention and procedure are the fruit of experience, and we owe them greater respect than the loose affiliations that seem to drive so much adaptability talk. And, we think, in high risk or exigent circumstances, improvisation is the last thing we need. Whether parachuting or planning a complex emergency response operation, lives hang in the balance. Surgery is no time for a brainstorm. But this is not what it means to be adaptable.

In his book *Learning from the Octopus*, Rafe Sagarin explores the ways that the DOD and DHS have created bureaucratic structures unable to respond rapidly to their threat environment. Part of his critique rests on comparing the predictive pursuits of security organizations to the adaptability of evolutionary systems within nature.

[340] Wallace Stegner, *The Sound of Mountain Water: The Changing American West*, (New York, NY:Knopf Doubleday Publishing Group, 2015), The Wilderness Letter.

Evolution, says Sagarin, “proceeds by solving survival problems as they arise. Many systems in society, by contrast, are littered with meticulously planned designed—the Maginot Line comes to mind—that were entirely unable to solve emerging threats from the environment.”[341] Organisms in nature survive without predictive knowledge because they have developed means of sensing and responding to changes in their environment. Many of the structures we put in place for the provision of security blunt our ability to respond to volatility in our environment. This is the danger of fortress thinking, and focusing on solidity over adaptability, or prediction over agility.

Unbounded risk makes such survival skills paramount. Assigned the unthinkable and the impossible, we are, in crucial and large-scale ways, we are responding with sclerotic, hardened tools designed for regularity.

The measure of success for a security policy, capability, or approach should not be its solidity, but its mutability, not its robustness, but it’s agility. “The problem is no longer about knowing the tools that help us to avoid surprises, but to train ourselves to be surprised.”[342] Adaptable security organization will look almost nothing like what we know, but will rely, thankfully, on skills we already possess.

Responders adapt. The rapid adaptation of utility trucks in hurricane Sandy to the requirements of airlift logistics illustrates the capacity of individuals to adapt when properly empowered and resourced to make and execute creative solutions. The question is whether the organizational systems we have in place augment or impede this adaptability.

The emphasis on adaptability is not mere iconoclasm, or barefoot philosophy. It requires active engagement with the changing nature of threats. The principle of adaptability relies on the nature of the risks that organizations confront. The emphasis and interest in adaptability is born from dangers of inertia—organizational arrangements incapable of sensing and responding to variable threat landscapes and methods that do

[341] Rafe Sagarin, *Learning From the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease* (New York: Basic Books, 2012), xxiii.

[342] Ibid.

not have the means to recognize that they are no longer effective. Organizational adaptability may mean that an entire organization will need to mobilize capabilities in response to an event nothing like their operational plan, and shift priorities based on its experience in that disaster. ICS and NIMS make this sort of movement difficult.

In the past several years, FEMA has focused on the development of rapidly deployable emergency response teams called Incident Management Assistance Teams (IMAT). IMATs are, "interagency, regionally based response teams that provide a forward Federal presence to improve coordination and response to serious incidents."[343] They train and deploy as small units to support emergency response efforts and coordinate the initial Federal role in support of disasters that may result in a Federal declaration. In effect, IMATs act as organizational sensors, establishing initial connections with impacted communities, and providing a means of rapidly assessing organizational requirements and operational impacts. The concept of IMATs, and the central role that they have played in recent FEMA response efforts illustrates a positive organizational trend towards developing smaller, more maneuverable teams that can act as adaptive drivers. The shift at FEMA towards the development and deployment of IMATs indicates a trend towards the kind of adaptive team environments that will allow for crisis management organizations to respond to the environments they operate in.

2. Pathfinding

> *Nowadays navigators rely so closely on technical aids that they find it much harder than the Western explorers of a couple of centuries ago to believe in primitive navigation. It is the very technical advancement in scientific navigation which has made the scientific navigators of today only too prone to build a wall of mystery, fable and myth around the natural navigators of the past.*
>
> —Harold Gatty[344]

[343] Federal Emergency Management Agency, "Fact Sheet, Incident Management Assistance Teams," Last Update June, 2014.

[344] Harold Gatty, *Finding Your Way Without Map or Compass* (Mineola, NY: Dover Publications, 2013), 34.

> *Of course, when the Naskapi do have information about the location of game, they tend to act upon it. Ordinarily, it is when they are uncertain and food supplies get low that they turn to their oracle for guidance.*
>
> —Omar Khayam Moore[345]

Charles Lindbergh called Harold Gatty the "prince of navigators." Gatty's unique interest was in the ability of "primitive" cultures to navigate successfully across uncharted landscapes; from the open ocean to the featureless expanses of the desert. In Greenland, Eskimo hunters carried carved wooden relief maps of the shoreline inside their mittens. Paddling in the dark, these maps allowed them to feel their way along a coastline rendered unfamiliar by the lack of light.[346]As an air force navigator, Gatty was familiar with and accustomed to the power of western navigational tools from compasses to charts, but he was equally interested in the dangers of over reliance upon technical aids. Too much reliance on technologies for navigation, reasoned Gatty, often resulted in navigators who quickly lost touch with navigational signals from their environments. When technical aids failed, this meant that navigators would be unable to navigate.

Pathfinding, or natural navigation, meant the cultivation of navigational skills based on observation and understanding of the environment—understanding that trees tend to extend their large limbs to the south, and paying attention to the flight of seabirds and the indications of seasonal changes.

In security, unbounded risk often places responders off of their existing maps. Catastrophe violates the rules of operational plans. The pre-established objectives and concepts of operation must adapt, and the individuals who respond must exhibit new skills for a changed environment. In such situations, pathfinding is a form of planning skill. For homeland security professionals this means cultivating skills for understanding threat environments that do not rely on the possession of perfect threat knowledge, or the capacity to relate catastrophic impacts to established plans.

[345] Omar Khayam Moore, "Divination-A New Perspective," *American Anthropologist, New Series*, 59, no. 1 (February 1, 1957): 69–74.

[346] L.B, "Eskimo Maps," *Imago Mundi* 5 (January 1, 1948): 92.

Henry the Navigator, the princely Portuguese explorer, "made his nation take a real interest in geographical discovery, broke down their superstitious fear of ocean sailing, and made a beginning in the circumnavigation of Africa."[347] Henry's leadership institutionalized exploration as a cultural value. At a time when, "sailors of the fifteenth century still feared the great perils which the passage of that Cape offered to their imagination," and the traditional belief of Arabic geographers in a "sea of darkness" permeated the thinking of most sailors, Henry approached the vast unknowns of the ocean with a very different ethic of exploration.[348]

Pathfinding is both an orientation to threats and hazards, and a better way of thinking about "coordination." As buzzwords go, "coordination" is among the more abused—used often enough to render homeland security almost senseless to its meaning. Pathfinding may serve as an ethic for organizations in security contexts to understand themselves and relate to others more effectively.

In response to the surge of unaccompanied minors on the southern border in 2014, the Secretary of DHS, at the direction of the President, initiated coordinated Federal action. In 2013, U.S. Customs and Border Protection (CBP) had "encountered over 24,000 unaccompanied children crossing the border. By May of [2014], the number has already doubled to just over 47,000." The surge of unaccompanied minors represented some uncharted organizational territory for homeland security. Recognizing that the capabilities of CBP and Immigration and Customs Enforcement (ICE) required assistance from other federal agencies, but lacking an existing operational construct for how such coordinated action should occur without a Stafford Act Declaration, DHS constructively resorted to pathfinding. CBP, ICE, DOD, Health and Human Services, and other agencies and departments were forced to address an uncommon response, and invent a paradigm for coordination. Command and control diminished in importance, as FEMA played the role of host, creating a forum for coordinating capabilities rather than an efficient

[347] Gomes Eannes de Zurara, *The Chronicle of the Discovery and Conquest of Guinea Vol. II,* translated by Charles Raymond Beazley and Edgar Prestage (New York, NY: Burt Franklin, 1899), cxii.

[348] Ibid., 313.

organization for executing centralized intent. FEMA’s National Response Coordination Center provided neutral territory, and the response occurred without unified command and control structures. Discovering solutions while operating off of maps and plans meant a different set of skills and expectations.

Crisis management expert Patrick Lagadec argues that increasingly, this kind of exploration is the norm for security organizations, and homeland security may require new capacity for understanding and making sense of “absurd” rather than “weak signals.” Lagadec describes this shift this way:

> We were trained to monitor “weak signals.” Now we must give priority to signals that cannot be noticed within the usual framework. It is not enough to magnify them in order to perceive and understand them. We need to openly question dormant variables, improbable combinations and contaminations, statistically insignificant events, and the convergence of intuitions. This means having additional sensibilities, new tolerance of ambiguities, different perceptions, and other tools.[349]

He is describing the predicament of the responder who must make sense of unfamiliar challenges and requirements. The need for this brand of pathfinding has not abated. The 2014–2015 Ebola outbreak illustrated that a public health emergency can rapidly acquire unforeseen characteristics. It was not simply a problem of public health monitoring, or the usual tools of pandemic; it was rapidly a problem of transportation infrastructure, border security, logistics and interagency coordination.

3. Mapmaking

Maps for unbounded risk will look drastically different than unconscionable maps. Planning for conditions of such uncertainty requires new skills, and a new form of map.

[349] Patrick Lagadec, “Risks and Crises in Terra Incognita,” *Paris Tech Review* (October 10, 2010).

a. The Shoulder Blade Path

"It should be remembered," says Omar Khayam Moore, "that it is difficult for human beings to avoid patterning their behavior in a regular way."[350] For the Naskapi tribes in Canada, breaking their cycles of regularity was a matter of survival. The Naskapi followed the caribou, and depended on hunting skills. But the caribou were an adaptive adversary, capable of responding to the movements of the Naskapi, and forcing the Naskapi to find means of being unpredictable. They turned to scapulimancy, a form of divination that relied on heating the shoulder blade of a caribou over a fire, and interpreting the cracks in its surface as auguries. Khayam Moore contends that this magical practice effectively randomized Naskai behavior, and served them as a tool for operating in conditions of uncertainty, outwitting their prey. As a response to a volatile risk, the Naskapi present some challenges to our current approach to security.

"Would it not be sounder practice," asks Moore, "for them simply to decide where, in their best judgment, game may be found and hunt there? Of course, when the Naskapi do have information about the location of game, they tend to act upon it. Ordinarily, it is when they are uncertain and food supplies get low that they turn to their oracle for guidance."[351] This is an important comparison with the way that homeland security manages risks. For risk management in situations where we possess sufficient knowledge to exert control, we do not need a new form of map making. But for unbounded risks, a different approach to knowledge and action may be warranted. "Like all people," says Moore, "[the Naskapi] can be victimized by their own habits…"[352]

The shoulder blade augury provided the Naskapi with a "chance like" instrument, a means of making themselves inscrutable to the adaptable caribou. "It seems safe to assume," says Moore, "that human beings require a functional equivalent to a table of random numbers if they are to avoid unwitting regularities in their behavior which can be

[350] Ibid.

[351] Moore, Omar Khayyam, "Divination-A New Perspective," *American Anthropologist, New Series,* 59, no. 1 (February 1, 1957): 69–74.

[352] Ibid.

utilized by adversaries."[353] Learning from the Naskapi means that planning for unbounded risks will require a different methodology. Plans for catastrophe and uncertainty may require less scripted knowledge, not more.

b. Fake Book Plans

In the world of jazz performance, "a fake-book is a bound collection of lead sheets...a musical score that shows only the melody of a work, usually written in treble clef, and its essential harmonic structure, usually indicated by alphanumeric symbols or tablature, or both, placed immediately above or below a single staff"[354] Fake books were the minimum necessary information about a song. Armed with fake books, jazz musicians could easily play the standards, and play them together. But the ultimate form of the song and the solos would depend on the circumstance.[355]

Fake books are form of melodic and harmonic crisis planning. Jazz performance relies on the interplay and communication between musicians as they improvise their way through a common theme. The results are unpredictable, and the essentials of the performance rely equally on the individual and technical proficiency of the musician, and his ability to keep time and communication with the rest of the band. The written music for such unpredictable environments necessarily takes a form quite different from classical symphonic notation. "Not only is jazz notation nearly impossible, but the very process would destroy the jazz spirit of spontaneous improvisation."[356]

It is axiomatic that plans do not survive first contact with the enemy. Equally, we are told that plans are nothing but planning is everything. This is the folk wisdom of planning, and it acknowledges that plans do not reflect the reality of operations, but rather

[353] Ibid.

[354] Rebecca Koblick, "Jazz fake-books as a resource in the general library," *Collection Building* 32, no. 4 (2013): 139-144.

[355] Fake books were also subversive documents. The best of them were illegally produced in violation of copyright, providing basic information about a wide range of musical numbers.

[356] D.R. Kulp, "The positive approach to teaching jazz," *Music Educators Journal*, Vol. 43, no. 3 (1957): 38-41.

that the exercise of planning is its own form of preparedness. This brand of thinking should protect the practice of planning from the production of unconscionable maps—maps that do not know they are maps. How well do such adages protect homeland security's mapping impulses?

The State of Nebraska Emergency Operations Plan 406 pages long.[357] As a map of every action necessary for responding to an emergency, this is certainly far too short. As an operational guide for responders or community members involved in an emergency it is perhaps too long. Nor is the plan's length unique. The State of Vermont's Emergency Operations Plan consists of a base plan, 60 annexes (covering State support functions, State agencies, support topics, and incident types) and 5 appendices.[358] This is common, and reflects a truth. Organization's emergency operations are immensely complicated. It also reflects the unconscionable mapping impulse.

The thinking, as it goes, is that the detailed operational plan will help build capability, test capability through exercises and then allow the organization to adapt and build the necessary structures indicated by the exercise in imagination that the plan represent. The limitation to this thinking is the over-commitment to a possible future. It is the proverbial problem of the Maginot line. Operational plans with this degree of specificity and task delineation have committed to a certain future. And such commitment represents a liability in a world of volatility. Operational planning for catastrophe and surprise requires some renovation then. The doctrine of multivalence may require "fake book planning" as an operational paradigm and discipline.

[357] Nebraska Emergency Management Agency, *State of Nebraska Emergency Operations Plan*, Lincoln, NE: Nebraska Emergency Management Agency, Updated November, 2014.

[358] Vermont Emergency Management and Homeland Security, *Vermont State Emergency Operations Plan*, 2013.

4. Reconciling

Why can't our dreams be content with the terrible facts?
The only animal cursed with responsible sleep,
We trace disaster always to our own acts.

—William Meredith, from "The Wreck of the Thresher"[359]

Multivalence requires homeland security organizations to adopt a new attitude about danger. Organizations that manage unbounded risks should reconcile themselves to uncertainty and accident.

On April 10th, 1963 the USS Thresher, the Navy's most advanced nuclear attack submarine, was lost at sea, taking with it all 129 crew members who perished in 8,400 feet of water off the coast of Cape Cod. Fifty years later, the cause the accident remains uncertain. The official explanation of the accident was couched with phrases such as "most probable" and "most likely," but settled on a faulty joint in a seawater pipe near the engine room.[360] The circumstances and available information are complex. But, according to most recent accounts, evidence supports a very different theory of cascading failure in electric busses, coolant pumps and a suddenly scrammed reactor.[361]

Testifying before Congress after the disaster, Vice Adm. H.G. Rickover, who was head of the Navy's nuclear propulsion program at the time of the accident approached the problem of catastrophe in the face of scant facts and complex organizational and technological problems with surprising wisdom:

> Statements have been made that [classified] the ship lost propulsion. Such statements cannot, in my opinion, be substantiated and may cause us to lose sight of the basic technical and management inadequacies that must be faced and solved if we are to do all we can to prevent further Thresher disasters…It is not the purpose of my testimony here today to prove that the nuclear power plant did not contribute to this casualty. When fact,

[359] William Meredith, *Effort at Speech: New and Selected Poems* (Evanston, IL: Northwestern University Press, 1997), 65.

[360] "50 Years Later, a Look at What Really Sank the Thresher," *Navy Times*, Accessed August 5, 2015, http://archive.navytimes.com/article/20130404/NEWS/304040021/50-years-later-look-what-really-sank-Thresher.

[361] Ibid.

> supposition, and speculation which have been used interchangeably are properly separated, you will find that the known facts are so meager it is almost impossible to tell what was happening aboard the Thresher at the critical time.[362]

We might glean from this a theory of forensic humility when faced with security problems where danger and management structures collide. With its cause still unknown, the wreck of the Thresher was the genesis for the Navy's SUBSAFE program, a system of revised safety certification practices for submarine design and testing.[363]

Meditating on the loss, former Naval aviator turned poet William Meredith concludes his account of the accident this way:

> Whether we give assent to this or rage
> Is a question of temperament and does not matter.
> Some will has been done past our understanding,
> Past our guilt surely, equal to our fears.[364]

It is a bleak thought, heavy with a view of the world's dangers as an ocean whose depths we cannot plumb. To Meredith's grieved thinking it hardly matters whether we accept or fight such forces. This is too heavy-hearted for homeland security, but combined with the bold humility of Adm. Rickover's disciplined uncertainty, it may provide a useful approach to complexity, uncertainty and danger.

In an important sense, the complexity of the Thresher—the design and fabrication of its systems, the management and quality control structures governing its construction, and the operational arrangements surrounding its deployment and testing–were beyond the ability to foresee its failure. And yet, as Meredith says, we always trace disaster to our own acts.

[362] Hearings before the Joint Committee on Atomic Energy Congress of the United States. Eighty Eighth Congress, First and Second Sessions on the Loss of the U.S.S. "Thresher," July 26, 27, July 23, 1963, and July 1, 1964 (Statement of Admiral Hyman G. Rickover).

[363] Hearing before the Committee on Science House of Representatives, One Hundred Eighth Congress, First Session, October 29, 2003 (Statement of Rear Admiral Paul E. Sullivan, U.S. Navy Deputy Commander for Ship Design, Integration and Engineering Naval Sea Systems Command).

[364] William Meredith, *Effort at Speech: New and Selected Poems* (Evanston, IL: Northwestern University Press, 1997), 65.

Uncertainty, and failures beyond our capacity should help us rethink our organizational arrangements with a kind of suspicion. This should encourage us to tinker and shift and fix. It should make us humble as we work to provide security. The enduring uncertainty that surrounds the Thresher accident is illustrative. Even imagining a future when we can confirm, finally and indisputably, the cause of the Thresher, we have already responded to the accident. We have already made decisions in the wake of a terrible accident. This has meant organizational changes, new programs, safety concepts doctrines, procedures and adaptations—all in the absence of certainty.

Worst cases should make organizations humble, says Lee Clarke.[365] During times of crisis and catastrophe, notes Clarke, America turns to and relies on organizations because they are able to command greater resources and tackle larger problems that individuals acting alone. But worst cases and unbounded risk mean that homeland security agencies need to acquire greater honesty about their limitations. Reconciling homeland security to unbounded risk means no longer promising levels of safety and security that are beyond the reach of organizations.

C. ORGANIZING FOR UNBOUNDED RISKS

"Huge, concentrated bureaucracies are unlikely to fail gracefully," says Lee Clarke.[366] The centralization of function, and the construction of more and more efficient management processes means that disruptions in the system of bureaucratic management are easily multiplied across a tightly coupled organization. And yet, as argued in this thesis, the trend in national preparedness planning and operations is toward more national uniformity, and the creation of huge, concentrated, ad hoc bureaucracies that span geographic boundaries and political jurisdictions.

The war fighting doctrines of the United States Army have begun to respond to the evolving nature of risks. Writing in 2012 on the behalf of the Joint Chiefs of Staff, General Martin Dempsey contended that the joint operations environment into the year

[365] Clarke, *Worst Cases*, 181.

[366] Ibid., 169.

2020 will be dynamic, fast paced, and volatile.[367] Responding in a, "competitive and interconnected world" means responding to an expanding list of asymmetric threats that span borders and challenge established doctrines.[368] This reality, according to Dempsey, calls for a corresponding evolution in military doctrine toward mission command. Briefly summarized, mission command is the decentralized execution of military missions.[369] Departing from the older, Westphalian model of military campaign management, mission command provides a more nimble, variable structure that delegates considerable responsibility and improvisational authority to the level of subordinate commanders, encouraging initiative across echelons.

Within the concept of mission command, "the commander is the central figure."[370] However, evaluating the accelerating changes in an increasingly interconnected world of threats, Dempsey concludes that smaller, lighter forces operating in an environment of increased uncertainty, complexity and competitiveness will require freedom of action to develop the situation and rapidly exploit opportunities. Decentralization will occur beyond current comfort levels and habits of practice."[371]

Retired General Stanley Mcchrystal recognized a similar change in the environment of war, and argues for a corresponding change in the organizational approach to operations, teamwork and leadership. In *Team of Teams*, Mcchrystal considers the organizational imperatives that follow unbounded risks. Volatile risks required a shift from the traditional model of military organization toward a more decentralized approach. Managing this decentralized approach, rather than permitting a detached form of leadership, required Mcchrystal to be differently, but more engaged.

[367] Dempsey, Martin E/General, U.S. Army/Chairman of the Joint Chiefs of Staff, "Mission Command: White Paper," April 3, 2012.

[368] Ibid.

[369] Department of Defense, *Joint Publication 3-0 "Joint Operations"* (Washington, DC: August, 11, 2011), II-2.

[370] Dempsey, Martin E/General, U.S. Army/Chairman of the Joint Chiefs of Staff, "Mission Command: White Paper," April 3, 2012.

[371] Ibid.

Adopting an, "eyes on, hands off" approach, Mcchrystal managed Joint Special Operations Command not in the manner of an omniscient leader moving chess pieces on a board, but as a gardener, creating the conditions for coordination between teams. Managing and cultivating a "Team of Teams" approach required a shift towards organizational transparency, shared consciousness and self-knowledge.

But homeland security has doubled down on scientific management as a means for crisis response, emergency management, and national incident management. In the face of unbounded risk, we have continued an investment in NIMS and ICS that presupposes an outcome of national uniformity. I have argued in this thesis that such uniformity is illusory and unattainable. It is also a liability—eliminating diversity in favor of regularity, but rendering emergency management organizations insensitive and slow to respond to changes by reducing operational elements to efficient executors of centrally defined functions within a larger system.

Rather, homeland security may require something other than a common tongue or structure. "Over time," says Gary Hart, "closed systems produce fewer and fewer innovations, because closed systems by definition are based on certain increasingly unchallengeable fundamental principles."[372] As the risk environment around NIMS challenges the fundamental assumptions of its structured approach, and undermines aspects of its principles, the concept of a national incident management system (enforced through the passive means of grant eligibility) is decreasing the innovative capacity of homeland security by attempting to establish such a closed system. The system of unbounded risks is open.

D. RESISTING UNIFORMITY: THE FORTRESS OF FEDERALISM

American government is a tangled system of overlapping authorities and spheres of responsibility. In a tactical sense, this creates enormous challenges around interoperability and coordination for crisis management. But perhaps, paradoxically, that

[372] Rafe Sagarin, *Learning From the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease* (New York, NY: Basic Books, 2012), ix.

makes America much safer. James Madison concludes Federalist No. 39 by examining the differences between the exercise of national power, and the structuring of that power under a federal model:

> The proposed Constitution, therefore, is, in strictness, neither a national nor a federal Constitution, but a composition of both. In its foundation it is federal, not national; in the sources from which the ordinary powers of the government are drawn, it is partly federal and partly national; in the operation of these powers, it is national, not federal; in the extent of them, again, it is federal, not national; and, finally, in the authoritative mode of introducing amendments, it is neither wholly federal nor wholly national.[373]

The paper itself has a greater elegance than this summary suggests. Taken as a whole, No. 39 in the series of published papers that argued for the ratification of the Constitution provides one of the clearest summaries of the essential character of Federalism, with Madison exploring the difference between a national and a federal government:

> In the former case, all local authorities are subordinate to the supreme; and may be controlled, directed, or abolished by it at pleasure. In the latter, the local or municipal authorities form distinct and independent portions of the supremacy, no more subject, within their respective spheres, to the general authority, than the general authority is subject to them, within its own sphere.[374]

American government was to be national in the operation of its powers (applying to every American), but federal in the extent of those powers (limited and enumerated in its powers). Emergency managers will recognize this principle reflected in the structure of Presidential Disaster Declarations made under the Stafford Act, which requires that, "All requests for a declaration by the President that a major disaster exists shall be made by the Governor of the affected State."[375]

[373] Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers* (Mineola, NY: Dover Publications, 2014), 186.

[374] Ibid.

[375] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, 1988 as amended, and 42 U.S.C. 5121-5207.

This principle is replicated across the homeland security enterprise. Federal and non-federal coordination is a dominant theme in advancing the provision of domestic security. And we recognize the struggle in its failures. Central to the *9/11 Commission Report* recommendations was the call for interoperable communications and unified incident command structures.[376] Hesitance on the part of the Federal government influenced the Post-Katrina Emergency Management Reform act. More recently, after action reporting on the 2013 Navy Yard shooting in Washington, DC concluded that local and federal law enforcement failed to share key pieces of information such as the availability of live video within the building.[377]

These failures make simplicity appealing. They seem to support an argument for more uniformity in operational capability, but perhaps also a more national approach to domestic crisis management. Perhaps they even suggest that the U.S. would be better served by a single domestic preparedness agency. At the very least, they suggest that aspects of Federalism are modern security liabilities. In the bargain of individual liberty we've purchased a form of insecurity, which works against a reliable governmental response to danger and threat.

But perhaps the opposite is true. Federalism is a great deconcentrator. Inherent in the maddening challenges of interoperability is a kind of modularity that distributes strengths along with vulnerabilities. State, local, tribal, community and individual responsibilities produce an inherent redundancy and an inherent distribution of vulnerability. This mirrors Charles Perrow's observation:

> We will never do well with prevention, remediation, and recovery from natural, industrials/technological, and terrorist disasters. Our organizations and our political system are simply not up to it. The best we can do is to reduce the size of the targets of nature's wrath, industrial errors, and terrorist attacks. The vast disaster literature rarely examines the

[376] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 397.

[377] Metropolitan Police Department of Washington DC, *After Action Report Washington Navy Yard September 16, 2013 Internal Review Of The Metropolitan Police Department* (Washington, DC: July 2014), 53.

> possibilities of deconcentrating populations in risky areas, hazardous materials concentrations, and reducing the power of the huge organizations that sit astride our critical infrastructure. We should reduce our vulnerabilities by reducing the size of that which is vulnerable.[378]

Federalism may be the ultimate antifragile system of government. But current approaches in NIMS and ICS work against it. Homeland security professionals have pursued national uniformity, and attempted to establish increasingly broad theatres of unified command, recognizing that the universality of doctrine, and the separation of federalism impede one another in cross-jurisdictional incidents. Perhaps a reorientation is in order.

Federalism was and remains a system uniquely designed to resist uniformity. If homeland security can remember how to engage it, our national network of governance is a system highly suited to adaptability and innovation.

1. The End of Disciplines: Interstitial Security

Unbounded risk presents daunting challenges to the science and practice of risk management, as well as the efficient models of command and control and the uniformity doctrines of NIMS. But it does not undermine them altogether.

Risk is still the essential underpinning of modern society, and managing risk is still effective in the large scale and over time. The challenge of homeland security is the management of outliers. For this reason, the focus of security organizations must evolve to be less concerned with the centralization of specific practices, and more about understanding and building systems that permit strangers to work with strangers more effectively.

This is a different set of skills, and the focus of this kind of security is about managing the connection points between practices and cultures. Decentralized risks, and network centric, federal structures require an approach to homeland security disciplines that is about managing the connections of the network, not simply the nodes. The central

[378] Charles Perrow, “Complexity, Catastrophe, and Modularity,” *Sociological Inquiry* 78, no. 2 (May 2008): 162–73.

task of homeland security management and organizational design becomes less about the establishment of organizational efficiency, and more about the creation of systems which are increasingly aware of themselves, and able to adapt and incorporate other systems.

I call this “interstitial security.” The doctrine of multivalence requires an interstitial approach that is homeland security at the borders of disciplines. It is about establishing means to connect fire and police, bomb squad and geospatial risk analyst. Rather than command and control organizations, we might argue that domestic security particularly requires the opposite: a domestic crisis response architecture focused on the uncommon partner. Because the problems of unbounded risk cut across artificial distinctions between political boundaries and disciplines, the necessary organizational response cannot be centralized with a specific discipline or capability.

2. Consider the Mouse

Conservative estimates on the losses associated with Australia’s 1993 mouse plague are upwards of AU$64.5 million.[379] And the losses have a cyclical, probabilistic cycle as well, observed to be around once every four years.[380] Mouse plagues do not occur on the same scale in the US, although there are interesting parallels between the governmental approach to managing pest animal outbreaks and some of the other disaster aid management programs available in the US.

In addition to being an enormous economic stress on rural agricultural areas, mouse plagues are difficult to predict and manage. Scientists have difficulty monitoring mouse population densities during and before the growing season.[381] Often the onset of the plagues is so sudden, it is not recognized as a plague until the mouse population has reached plague numbers, creating challenges for those who have to respond with mouse

[379] Peter R. Brown, et al., *Rodent Outbreaks: Ecology and Impacts* (Metro Manilla, Phillipines: IRRI, 2010), 225.

[380] Ibid.

[381] Ibid.

bait, and even creating shortages in mouse bait.[382] In one instance a month long backlog of mouse bait highlighted that entire crops can be lost in the span of days, while farmers waited for the delivery of poison for weeks.[383]

In 2011 the government of south Australia convened and responded to recommendations from a "state mouse working party" on how to provide a better framework for delivering governmental assistance to farmers. The recommendations are interesting, and parallel many of the challenges of U.S. management of complicated risks between public and private sector interests, and encouraging private investment to manage public risks.

The recommendations include regulatory relief for farmers to be able to mix pesticides on their own property, easing licensure requirements for specialists who mix the zinc phosphide bait into the soil, and other means of improving knowledge and application of baiting technology in rural areas. In addition, the recommendations tackle an interesting issue of biosecurity—identifying methods and mechanisms by which to collect and transmit agricultural intelligence products on the state of mouse populations and their potential threat to the environment.[384]

There are significant lessons that the U.S. can learn in terms of establishing and being ready to repurpose intelligence architecture to respond to weird threats and hazards. In particular, the U.S. learned this lesson during the 2014 Ebola outbreak, as public health threats highlighted the need to provide medical intelligence to CBP.

[382] Government of New South Wales, Department of Primary Industries, "Early detection of mouse plagues," Primefact 505, Second edition, September 2013.

[383] Herbert, PM Bronwyn, "Four-State Mouse Plague Eating at Bottom Line," ABC News, June 17, 2011.

[384] Primary Industries and Regions South Australia, "Declared Animal Policy under the Natural Resources Management Act 2004: house mouse (Mus musculus)," June 11 2013.

E. CONCLUSION

> *I dream'd in a dream, I saw a city invincible to the attacks of the whole of the rest of the earth*
>
> —Walt Whitman[385]

Faced with expanding uncertainty, security agencies have sought expanded rationality. Faced with complexity, security agencies have sought regularity. Wrestling with disparate arrangements across jurisdictions and sectors, security efforts have sought to build national uniformity. However, uncertainty endures, complexity seems inevitable, and American government was designed specifically to resist the centralization of efficient power, uniform national systems of crisis management, or the centralized command of resources during disasters. It is the inherent nature of unbounded risks to defy efforts at uniformity and control. In one sense, this is simply to recognize that the margin of what remains unknown is of particular import to homeland security agencies and efforts. The unlikely rail accident, the unthinkable airline crash, and the worst-case earthquake or pandemic is specifically the province of agencies and organizations responsible for national preparedness. Perfect security remains, as the poet Walt Whitman saw it, a dream.

However, the national capabilities and approaches currently in use are not optimized for the management of outliers, or for living with unbounded risks. Designed around assumptions of threat, vulnerability, and consequence, the architecture of homeland security decision-making is less attuned to situations where this information is unavailable. The establishment of efficient incident management organizations occludes the means of perception necessary to make sense of incident complexity. The necessary repurposing of intelligence means and methods to work with uncommon partners during pandemics, or other volatile threats are impeded by current precautionary approaches. The dominant modes of planning build detailed task objectives, task lists, and maps for

[385] Walt Whitman, *Leaves of Grass Including a Facsimile Autobiography, Variorum Readings of the Poems and a Department of Gathered Leaves*, Edited by David McKay (Philadelphia, US: David McKay, 1891-1892), 109.

incidents that inevitably unfold differently. In this environment it is difficult to know how much safer security efforts make America.

This does not mean the end of risk management. Unbounded risk should teach security agencies and professionals to cultivate a new set of skills alongside traditional risk management practices, specifically designed for the management of uncertainty, threat, and worst-case catastrophe. This suggests a conclusion in two parts—one incremental, the other more dramatic.

1. Incremental Recommendation

Multivalence and national adaptability are characteristics that can augment current security practices. Patrick Lagadec's concept of a "rapid reflection force" is an example of the way in which this kind of thinking can be brought in not to override or change existing practice but to augment and support existing practice with the kind of thinking that unbounded risk requires. This is not limited to incident management, but should also pervade the way that security organizations approach planning, the review of policy and the development of procedures. In this thesis I have proposed four aspects to multivalence, and the cultivation of these capacities alongside existing security processes may improve security sensitivity to volatile and uncertain risk. The Lac-Mégantic rail accident, and the challenges of providing insurance controls for terrorism risk highlight necessary incremental adaptations to unbounded risks. Security organizations must orient themselves more fully to the unknown.

2. Thoroughgoing Changes

Unbounded risk suggests the need for drastic changes. Reconfiguring planning practices to produce "fake book" plans—plans that did not attempt to predict future conditions but instead provided a common framework for improvising in uncertainty—would mean dramatic changes in a culture that demands and produces unconscionable maps. This thesis suggests that such adaptability planning is more useful to the security professional, but as Lee Clarke has argued, it is important to understand that plans—as maps that do not just guide operations but also communicate to organizations and citizens—serve more than merely practical purposes. Implementing this change would mean fewer plans that propose a grand design. Recognizing that organizations are directed to produce grand operational plans, this means a shift in the political expectation for such plans, not simply the operational impulse to produce them.

The reassertion of American federalism against the tide of national uniformity is no less drastic. This thesis suggests that the impediments to achieving national uniformity have not been greatly reduced, merely disguised by existing efforts to produce a national incident management system. The skills still wanting for achieving interoperability and effective joint efforts across jurisdictions, it seems, have less to do with the establishment of a common system, and more to do with an improved ability to work effectively with strangers, and to navigate the complex networks of risk and governance.

Centralization and efficiency have a curious revenge effect—they also create vulnerabilities. Understanding that the tragedy of Germanwings 9525 was made possible by robust, complicated fortifications means recognizing that the centralization, even of strengths, makes room for unbounded risk. Finding and cultivating means to distribute both vulnerabilities and strengths means a broad, national effort at dismantling criticalities that come with complex systems. But unbounded risks suggest that just such drastic undertakings are necessary in order to push back against catastrophic possibilities—from climate disaster to terrorist attack. Abandoning the pursuit of NIMS, or the command and control doctrines of ICS is an unlikely proposition, and yet the dynamic nature of modern risk may require it.

American government is uniquely structured to adapt to dynamic risks, and equally to resist nationally uniform security measures. A grand design for homeland security will not produce grand security. Rather, improved security may rest on the staggered strengths of federalism and the management of connections in a security network.

The end of homeland security may be to manage the unmanageable. This means both navigating without maps, and making maps for uncharted waters. Organizationally, inheriting unbounded risk may mean turning away from the manufactured insecurities that accompany unconscionable maps, and toward a better means of living with danger.

It is likely that adaptable, decentralized systems will make America safer. Rather than embracing organizational doctrine meant to impose artificial command and control, federalism needs a security rebirth. Homeland security needs fewer scripted plans and more improvisation, more diversity, less uniformity, less training with partners and more learning to work with strangers. These things will make us safer, but they will not make us safe.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Acker, P., and C. Larrington. *The Poetic Edda: Essays on Old Norse Mythology*. Garland Medieval Casebooks Series. London, UK: Routledge, 2002.

Adam, Barbara, Ulrich Beck, and Joost Van Loon. *The Risk Society and Beyond: Critical Issues for Social Theory*. London, UK: SAGE, 2000.

Akerman, James R. and Robert W. Karrow. *Maps: Finding Our Place in the World*. Chicago, IL: University of Chicago Press, 2007.

American Institutes for Research. *The Evaluation of the National Flood Insurance Program Final Report*. Washington, DC: October, 2006.

Aradau, Claudia, and Rens Van Munster. "Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future." *European Journal of International Relations* 13, no. 1 (2007): 89–115.

———. *Politics of Catastrophe: Genealogies of the Unknown*. London, UK: Routledge, 2011.

———. "The Securitization of Catastrophic Events: Trauma, Enactment, and Preparedness Exercises." *Alternatives: Global, Local, Political* 37 (2012).

———. "The Time/Space of Preparedness: Anticipating the 'Next Terrorist Attack.'" *Space & Culture* 15, no. 2 (May 2012): 98–109.

Aristotle. *Physics*. Translated Robin Waterfield and David Bostock. Oxford, UK: Oxford University Press, 1999.

Barkun, Michael. "Defending Against the Apocalypse: The Limits of Homeland Security." *Policy Options* (September 2002).

Beck, Ulrich. "Living in the World Risk Society." *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

———. *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt, DE: Suhrkamp Verlag, 1986.

———. *Risk Society: Towards a New Modernity*. London, UK: SAGE, 1992.

———. "The Terrorist Threat World Risk Society Revisited." *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

———. *World at Risk*. New York, NY: Wiley, 2013.

Belloc, Hilaire. *The Bad Child's Book of Beasts.* London, UK: Duckworth, 1896.

Berman, Paul. *Terror and Liberalism*. New York, NY: W.W. Norton & Company, 2004.

Bernstein, Peter L. *Against the Gods: The Remarkable Story of Risk*. New York, NY: John Wiley & Sons, 2012.

Bice, William B. "British Government Reinsurance and Acts of Terrorism: The Problems of Pool Re." *U. Pa. J. Int'l Bus. L*. 15 (1994): 441.

Birkland, Thomas A., and Sarah E. DeYoung. "Emergency Response, Doctrinal Confusion, and Federalism in the Deepwater Horizon Oil Spill." *Publius: The Journal of Federalism* 41, no. 3 (July 1, 2011): 471–93.

Bismarck, Otto Von . *Fürst Bismarck: neue Tischgespräche und Interviews* [prince Bismarck: new table discussions and interviews]. Stuttgart and Leipzig, DE: Deutsche Verlags-Anstalt, 1895, 248.

B., L. "Eskimo Maps." *Imago Mundi* 5 (January 1, 1948): 92.

Boin, Arjen, and Patrick Lagadec. "Preparing for the Future: Critical Challenges in Crisis Management." *Journal of Contingencies & Crisis Management* 8, no. 4 (December 2000): 185.

Boin, Arjen, Patrick Lagadec, Erwann Michel-Kerjan, and Werner Overdijk. "Critical Infrastructures under Threat: Learning from the Anthrax Scare." *Journal of Contingencies & Crisis Management* 11, no. 3 (September 2003): 99–104.

Borges, Jorge Louis. *Jorge Luis Borges. Collected Fictions*. Translated by Hurley, H. New York, NY: Penguin Books, 1998. 235.

Bray, Olive, trans. *The Elder or Poetic Edda-Commonly Known as Saemon's Edda*. London, UK: King's Weighouse Rooms, 1908.

Bredow, Interview Conducted by Rafaela von, and Veronika Hackenbroch. "Interview with Peter Piot Discoverer of the Ebola Virus." *Spiegel Online*, September 26, 2014.

Bronowski, J. "The Creative Mind," *Scientific American, Art In Science*. Simon and Schuster Inc. 1954.

Brown, Peter R., Grant R. Singleton, Roger P. Pech, Lyn A. Hinds, and Charles J. Krebs. and International Rice Research Institute. *Rodent Outbreaks: Ecology and Impacts*. Metro Manilla, Phillipines: IRRI, 2010.

Buck, Dick A., Joseph E. Trainor, and Benigno E. Aguirre. "A critical evaluation of the incident command system and NIMS." *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006).

Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile (BEA). *Rapport préliminaire Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l'Airbus A320-211 immatriculé D-AIPX exploité par Germanwings.* Paris, FR: BEA, May 2015.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Pub., 1998.

Carroll, Lewis, and Harry Furniss. *Sylvie and Bruno Concluded*. New York NY: Macmillan and Co., 1893.

Caudle, Sharon. "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community." *Homeland Security Affairs* 1, Article 2 (August 2005).

Clarke, Lee. *Mission Improbable: Using Fantasy Documents to Tame Disaster*. Chicago, IL: University of Chicago Press, 1999.

———. *Worst Cases: Terror and Catastrophe in the Popular Imagination*. Chicago IL: University of Chicago Press, 2006.

Coker, Christopher. *Globalization and Insecurity in the Twenty-First Century*. Oxford, UK: Oxford University Press for the International Institute for Strategic Studies, 2002.

Conrad, Joseph. *The Secret Agent: A Simple Tale*. New York, NY: Doubleday, Page & Company, 1916.

Davis, Jack. "Sherman Kent and the Profession of Intelligence Analysis." *The Sherman Kent Center for Intelligence Analysis, Occasional Papers*: Volume 1, Number 5, Washington, DC: November 2002.

———. "Strategic Warning: If Surprise is Inevitable, What Role for Analysis?" *The Sherman Kent Center for Intelligence Analysis, Occasional Papers*: Volume 2, Number 1. Washington, DC: January 2003.

Deloitte & Touche LLP. *Committee of Sponsoring Organizations of Treadway Commission. Risk Assessment in Practice.* New York, NY: Deloitte & Touche LLP, October 2012.

Dempsey, Martin E. /General, U.S. Army/Chairman of the Joint Chiefs of Staff. "Mission Command: White Paper." Washington, DC: April 3 2012.

Department of Defense. *Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 January 2015). Washington, DC: 2015.

———. *Joint Publication 3–0. Joint Operations*. August 11, 2011.

Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013.

———. *National Response Framework, second edition*. Washington, DC: DHS, May 2013.

———. *The 2014 Quadrennial Homeland Security Review*. Washington, DC: DHS, 2014.

———. *U.S. Department of Homeland Security Agency Financial Report Fiscal Year 2014*. Washington, DC: DHS, February 2015.

———. *Response Federal Interagency Operational Plan*. Washington, DC: DHS, July 2014.

———. *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*. Washington, DC: DHS, December 2011.

———. *National Preparedness Goal, First Edition*. Washington, DC: DHS, September 2011.

———. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. Washington, DC: DHS, April 2011.

Department of Homeland Security, Office of the Inspector General. *FEMA and the State of Louisiana Need to Accelerate the Funding of $812 Million in Hazard Mitigation Grant Program Funds and Develop a Plan to Close Approved Projects*. Report. Washington, DC: DHS, September 2014.

Department of Homeland Security, Risk Steering Committee. *DHS Risk Lexicon 2010 Edition.* Washington, DC: DHS, September 2010.

Department of the Navy. *Command and Control (Marine Corps Doctrinal Publication 6)*. Washington, DC: U.S. Marine Corps, 1996.

———. *Report of the Investigation Into the Fatal Shooting Incident at the Washington Navy Yard on September 16, 2013.* Washington, DC: November 8, 2013.

Department of Transportation’s Pipeline and Hazardous Materials Safety Administration. “PHMSA - Chronology.” http://www.phmsa.dot.gov/hazmat/osd/chronology.

DeSilver, Drew. “U.S. Spends over $16 Billion Annually on Counter-Terrorism.” Pew Research Center. http://www.pewresearch.org/fact-tank/2013/09/11/u-s-spends-over-16-billion-annually-on-counter-terrorism/.

Duzer, Chet A. Van. *Sea Monsters on Medieval and Renaissance Maps*. London, UK: British Library, 2013.

Eagleton, Terry. *Sweet Violence: The Idea of the Tragic*. Hoboken, NJ: Wiley, 2009.

Ericson, Richard, and Aaron Doyle. “Catastrophe Risk, Insurance and Terrorism.” *Economy and Society* 33, no. 2 (2004): 135–73.

Erikson, Kai T. *A New Species of Trouble: The Human Experience of Modern Disasters*. New York, NY: W.W. Norton & Company, 1995.

Farissol, Abraham ben Mordecai, and T. Hyde. *Itinera Mundi Cum Interpretatione* [the ways of the world, with interpretation]. Ugolini’s Thesaurus Antiquitatum Sacrarum, 1747.

Federal Emergency Management Agency. *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101*. Washington, DC: FEMA, November 2010.

———. “New Position Paper on National Incident Management System (NIMS) Incident Command System (ICS) - Homeland Security Digital Library Blog.” Accessed April 16, 2015. http://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

———. “Fact Sheet, Incident Management Assistance Teams.” Last Updated June 2014.

———. “Build a Kit.” Accessed August 1, 2015. http://www.ready.gov/build-a-kit.

———. “Resource Typing Library Tool (RTLT)-v1.3.0.” Accessed August 1, 2015. https://rtlt.preptoolkit.org/Public.

———. *FEMA 320, Taking Shelter from the Storm: Building a Safe Room for Your Home or Small Business*. Washington, DC: FEMA, 2008.

———. *FEMA P-765, Midwest Floods of 2008 in Iowa and Wisconsin*. Mitigation Assessment Team Report, Washington, DC: FEMA, 2009.

———. *National Incident Management System*. Washington, DC: FEMA, December 2008.

———. “Release 101020: FEMA Administrator Craig Fugate Urges State Emergency Managers To Prepare For The Worst And Consider The Entire Community While Planning For Disaster, No.: HQ-10-203,” Washington, DC: October 20, 2010.

———. *Risk Management Series: Incremental Protection for Existing Commercial Buildings from Terrorist Attack*. Washington, DC: FEMA, April 2008.

———. *Nuclear/Radiological Incident Annex*. Washington, DC: FEMA, 2008.

———. *Hurricane Sandy FEMA After Action Report.* Washington, DC: FEMA, July 1, 2013.

Filip, Mark, Joseph Hagin, Danielle Gray, Thomas Perrelli. *Executive Summary to Report to the Secretary of Homeland Security*. Washington, DC: United States Secret Service Protective Mission Panel, December 15, 2014.

FIRESCOPE, “Operations Team Meeting.” Meeting minutes. Los Angeles County Fire Department, Lac Camp #2, March 30, 1987.

Forlani, Paolo. *Vniversale Descrittione Di Tvtta La Terra Conoscivta Fin Qvi* [a map of the world from 1565]. 1565.

Foucault, M., M. Bertani, A. Fontana, F. Ewald, and D. Macey. *“Society Must Be Defended”: Lectures at the Collège de France, 1975–1976. Lectures at the Collège de France*. London, UK: St Martins Press, 2003.

Foucault, Michel, Michel Senellart, François Ewald, and Alessandro Fontana. *Security, Territory, Population: Lectures at the Collège de France 1977—1978*. London, UK: Macmillan, 2009.

Fukuyama, Francis. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, DC: Brookings Institution Press, 2008.

Gardner, Robert Owen. “The Emergent Organization: Improvisation and Order in Gulf Coast Disaster Relief.” *Symbolic Interaction* 36, no. 3 (August 2013): 237–60.

Gatty, Harold. *Finding Your Way Without Map or Compass*. Mineola, NY: Dover Publications, 2013.

Gibson, Fiona. “Pool Re Must Wait for Answer on Funding.” *Lloyds List*. London, UK: December 15, 1993.

Gigerenzer, Gerd. “Dread risk, September 11, and fatal traffic accidents.” *Psychological science* 15, no. 4 (2004): 286–287.

Glennon, Michael. *National Security and Double Government*. Oxford, UK: Oxford University Press, 2014.

Guy Carpenter. *2015 Terrorism Risk Insurance Report*. Insights. Chicago, IL: Marsh and McLennan Companies, June 2015.

———. *Global Terrorism Report*. Chicago, IL: Marsh and McLennan Companies, 2014.

Hacking, I. *The Taming of Chance. Ideas in Context*. Cambridge, UK: Cambridge University Press, 1990.

Hamilton, Alexander James Madison, and John Jay. *The Federalist Papers.* Mineola, NY: Dover Publications, 2014.

Hartwig, Robert P. and Claire Wilkinson, *Terrorism Risk: A Constant Threat, Impacts for Proterty and Casualty Insurers*. Paper. New York, NY: Insurance Information Institute, March 2014.

Heaney, Seamus trans. *Beowulf (Bilingual Edition)*. New York, NY: W.W. Norton, 2001.

Heinlein, Robert A. *Time Enough for Love*. New York, NY: Penguin, 1987.

Hoffman, Bruce. *Inside Terrorism*. New York, NY: Columbia University Press, 2013.

Homeland Security Council. *National Planning Scenarios: Executive Summaries Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities*. Washington, DC: Homeland Security Council, April 2005.

Hubbard, Douglas W. *The Failure of Risk Management: Why It's Broken and How to Fix It*. New York, NY: John Wiley and Sons, 2009.

Huntingdon, Henry of. *The Chronicle of Henry of Huntingdon. Comprising the history of England, from the invasion of Julius Cæsar to the accession of Henry II. Also, The acts of Stephen, king of England and duke of Normandy*. Edited and translated by Thomas Forester. London, UK: H. G. Bohn, 1853.

Huysmans, Jef, and Anastasia Tsoukala. "Introduction: The Social Construction and Control of Danger in Counterterrorism." *Alternatives: Global, Local, Political* 33 (April 2008).

Interagency Security Committee. *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard.* Washington, DC: Interagency Security Committee, August 2013.

Jensen, Jessica. “The Current NIMS Implementation Behavior of United States Counties.” *Journal of Homeland Security and Emergency Management* 8, no. 1. (January 2, 2011).

Justinian. *The Digest of Justinian*. Translated by Charles Henry Monro, edited by William Warwick Buckland. Cambridge, UK: Cambridge University Press, 1909.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. Hudson Institute Series on National Security and International Order. Piscataway, NJ: Transaction Publishers, 2009 (originally published in 1965).

———. *Thinking about the Unthinkable*. New York, NY: Horizon Press, 1962.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York, NY: Doubleday, 2011.

Kaplan, Amy. “Homeland Insecurities: Some Reflections on Language and Space.” Radical History Review 85, no. 1 (2003): 82–93.

Kasperson, Roger E., Ortwin Renn, Paul Slovic, Halina S. Brown, Jacque Emel, Robert Goble, Jeanne X. Kasperson, and Samuel Ratick. “The social amplification of risk: A conceptual framework.” *Risk Analysis*, (1988) 8: 177–187.

Kent, Adrian. “A Critical Look at Risk Assessments for Global Catastrophes.” *Risk Analysis* 24, no. 1 (2004): 157–68.

Keynes, John Maynard . “The General Theory of Employment.” *The Quarterly Journal of Economics*, Vol. 51, No. 2 (Feb., 1937), pp. 209–223, Published by: Oxford University Press.

Koblick, Rebecca. “Jazz Fake-Books as a Resource in the General Library.” *Collection Building* 32, no. 4 (2013): 139–144.

Korzybski, Alfred. *Alfred Korzybski: Collected Writings, 1920–1950,* Edited by M. Kendig. Fort Worth, TX: Institute of GS, 1990.

Kulp, D.R. “The Positive Approach to Teaching Jazz.” *Music Educators Journal*,. Vol. 43, no. 3 (1957): 38–41.

Kunreuther, Howard, and Erwann Michel-Kerjan. *TRIA after 2014: Examining Risk Sharing under Current and Alternative Designs.* Philadelphia, PA: Wharton, University of Pennsylvania, 2014.

Lagadec, Erwan. *Unconventional Crises, Unconventional Responses: Reforming Leadership in the Age of Catastrophic Crises and Hypercomplexity*. Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Baltimore, MD: Johns Hopkins University, 2007.

Lagadec, Patrick. “A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice.” Review of Policy Research 26, no. 4 (2009): 473–86.

———. *La civilisation du risque: catastrophes technologiques et responsabilité sociale*. Paris, France: Seuil, 1981.

———. “Leadership in Terra Incognita – Mapping the Way for Senior Executives.” *Crisis Response Journal* 6, no. 3 (2010).

———. *Major Technological Risk: An Assessment of Industrial Disasters*. Oxford, UK: Elsevier Science Limited, 1982.

———. “Risks and Crises in Terra Incognita.” *Paris Tech Review*. (October 10, 2010).

Lewis, Ted. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: Wiley-Interscience, 2006.

London, Jack. *The Strength of the Strong.* New York, NY: Macmillan, 1914.

Macfarlane, Robert. *The Wild Places*. New York, NY: Penguin, 2008.

Magnus, Olaus. *Carta Marina et Descriptio Septemtrionalium Terrarum Ac Mirabilium Rerum in Eis Contentarum, Diligentissime Elaborata Annon Domini 1539 Veneciis Liberalitate Reverendissimi Domini Ieronimi Quirini*. 1532.

Mass, Todd, Siobahn O’Neil, and John Rollins. *The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. (CRS Report No. RL33858). Washington, DC: Congressional Research Service, 2007. http://www.fas.org/sgp/crs/homesec/RL33858.pdf.

McChrystal, Stanley, Tantum Collins, David Silverman, Chris Fussell. *Team of Teams: New Rules of Engagement for a Complex World*. New York, NY: Penguin Publishing Group, Kindle Edition, May 12, 2015.

Meredith, William. *Effort at Speech: New and Selected Poems*. Evanston, IL: Northwestern University Press, 1997.

Moore, Omar Khayyam. “Divination - A New Perspective.” *American Anthropologist, New Series,* 59, no. 1 (February 1, 1957): 69–74.

Morton, John Fass. *Next-Generation Homeland Security: Network Federalism and the Course to National Preparedness*. Annapolis, MD: Naval Institute Press, 2012.

Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. New York, NY: Free Press, 2006.

Mueller, John, and Mark G. Stewart. “Hardly Existential.” *Foreign Affairs*. (April 2, 2010).

———. *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. New York, NY: Oxford University Press, USA, 2011.

Muller, Richard. *Physics for Future Presidents: The Science Behind the Headlines*. New York, NY: W.W. Norton & Company, 2008.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York, NY: W.W. Norton & Company, 2004.

National Infragard EMP Special Interest Group. High Impact Threats to the Electrical Grid: Workshop and Tabletop Exercise. Washington, DC: Infragard, 2015.

National Oceanic and Atmospheric Administration. *NOAA 2012 Atlantic Hurricane Season Outlook*. Washington, DC: NOAA, issued May 24, 2012.

Nebraska Emergency Management Agency. *State of Nebraska Emergency Operations Plan*. Lincoln, NE: Nebraska Emergency Management Agency, Updated November, 2014.

Newton, Sir Isaac, Andrew Motte, William Davis, John Machin, and William Emerson. *The Mathematical Principles of Natural Philosophy*. London, UK: H.D. Symonds, 1803.

Ohio Emergency Management Agency. *Ohio Emergency Operations Plan, Base Plan*. Columbus, OH: Ohio Emergency Management, July 2014.

Oresme, Nicole. *Le Livre Du Ciel et Du Monde*. Madison, WI: University of Wisconsin Press, 1941.

Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. Princeton Paperbacks. Princeton, NJ: Princeton University Press, 1984.

———. “Complexity, Catastrophe, and Modularity.” *Sociological Inquiry* 78, no. 2 (May 2008): 162–73.

Petit, F. D., G. W. Bassett, W. A. Buehring, M. J. Collins, D.C. Dickinson, R.A. Haffenden, A.A. Huttenga, M.S. Klett, J.A. Phillips, S.N. Veselka. *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability.* Oak Ridge, TN: Argonne National Laboratory July 2013.

Poolre. “Pool Reinsurance Company Ltd.” Accessed March 14, 2015. https://www.poolre.co.uk/.

———. “Pool Re Purchases £1.8 Billion in Reinsurance.” Accessed March 9, 2015. https://www.poolre.co.uk/pool-re-purchases-1-8-billion-in-reinsurance/.

Posner, Richard A. *Catastrophe : Risk and Response*. Oxford, UK: Oxford University Press, 2004.

Postman, Neil. *The End of Education: Redefining the Value of School*. Vintage. New York, NY: Knopf Doubleday Publishing Group, 1996.

Quammen, D. *Monster of God: The Man-Eating Predator in the Jungles of History and the Mind*. New York, NY: W.W. Norton, 2004.

Rasmussen, Mikkel Vedby. “‘It Sounds Like a Riddle’: Security Studies, the War on Terror and Risk.” *Millennium - Journal of International Studies* 33, no. 2 (March 1, 2004): 381–95.

Rawls, John. *A Theory of Justice*. Boston, MA: Harvard University Press, 2009.

Rediker, Marcus. *Between the Devil and the Deep Blue Sea: Merchant Seamen, Pirates and the Anglo-American Maritime World, 1700–1750*. Cambridge, UK: Cambridge University Press, 1989.

Renaud, Cynthia. “The Missing Piece of NIMS: Teaching Incident Commanders How to Function in the Edge of Chaos.” *Homeland Security Affairs* 8, Article 8. June 2012.

Richard of Haldingham and Lafford. “Hereford Mappa Mundi.” 1285.

Risk Management Solutions. Quantifying U.S. Terrorism Risk. White Paper. Newark, CA: RMS, 2014.

Rogers, Paul. “Political Violence and Economic Targeting Aspects of Provisional IRA Strategy, 1992–97.” *Civil Wars* 3, no. 4 (December 1, 2000): 1–28.

Rosenburg, David. “Camouflage is a Conceptual Look at Snipers,” *Slate Magazine*, New York, US, January 20, 2015.

Safire, William. “On Language; Hermen Eutic’s Original Intent.” *The New York Times*, September 6, 1987, sec. Magazine.

Sagan, Scott D. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton Studies in International History and Politics. Princeton, NJ: Princeton University Press, 1995.

Sagarin, Rafe. *Learning From the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease*. New York, NY: Basic Books, 2012.

Seuss, Dr. *Oh, Say Can You Say?* New York, NY: Beginner Books, 1979.

Shakespeare, William. *A Midsummer Night's Dream.* Philadelphia: J.B Lippincott and Co., 1895.

Shah, Sameer. "Perception of Risk: Disaster Scenarios at Brookhaven." Paper. Boston, MA: Massachusetts Institute of Technology, 2003.

Percy Bysshe Shelley. *Prometheus Unbound: A Lyrical Drama in Four Acts*. London, UK: J.M Dent and Company, 1898.

Silverman, Hugh J., and Don Ihde. *Hermeneutics and Deconstruction. Selected Studies in Phenomenology and Existential Philosophy*. Albany, NY: State University of New York Press, 1985.

Slovic, Paul. "Perception of Risk." *Science* 236, no. 4799 (1987): 280–85.

———. *Smoking: Risk, Perception, and Policy*. London, UK: SAGE, 2001.

———. *The Perception of Risk*. London, UK: Earthscan Publications, 2000.

Sornette, Didier. "Dragon-Kings, Black Swans and the Prediction of Crises." *International Journal of Terraspace Engineering*, 2 (1), 1–18 (2009).

Stambler, Kimberly S, and Joseph A Barbera. "Engineering the Incident Command and Multiagency Coordination Systems." *Journal of Homeland Security and Emergency Management* 8, no. 1 (January 23, 2011).

Stegner, Wallace. *The Sound of Mountain Water: The Changing American West.* New York, NY: Knopf Doubleday Publishing Group, 2015.

Stewart, Stacy. *National Hurricane Center Annual Summary: 2012 Atlantic Hurricane Season.* Washington, DC: National Oceanic and Atmospheric Administration, January 23, 2014.

Sunstein, Cass R. *Laws of Fear: Beyond the Precautionary Principle*. John Robert Seeley Lectures. Cambridge, UK: Cambridge University Press, 2005.

———. "The Most Knowledgeable Branch." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 14, 2015.

———. "The Paralyzing Principle." *Regulation* 25, no. 4 (Winter 2002/2003 2002): 32.

———. *Worst-Case Scenarios.* Boston, MA: Harvard University Press, 2007.

Taylor, Frederick Winslow. *The Principles of Scientific Management.* New York, NY: Harper, 1913.

Taleb, Nassim Nicholas. *Antifragile: Things That Gain from Disorder.* New York, NY: Incerto Series, Random House, 2012.

———. *The Black Swan: The Impact of the Highly Improbable*. New York, NY: Random House Publishing Group, 2007.

Taleb, Nassim Nicholas, Rupert Read, Raphael Douady, Joseph Norman,Yaneer Bar-Yam. "The Precautionary Principle (with Application to the Genetic Modification of Organisms)." *Extreme Risk Initiative*. New York, NY: NYU School Of Engineering Working Paper Series September 2014.

Teeter, Andrew C. "On A Clear Day, You Can See ICS: The Dying Art Of Incident Command And The Normal Accident Of NIMS—A Policy Analysis." Master's thesis, Naval Postgraduate School, March 2013.

Transportation Safety Board of Canada. *Railways Investigation Report R13D0054: Runaway and Main-Track Derailment of Montreal, Maine, & Atlantic Railways Freight Train MMA-002 MILE 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013*. Gatineau, QC: August 2014.

U.S. Global Change Research Program. "National Climate Assessment." National Climate Assessment. Accessed July 1, 2015. http://nca2014.globalchange.gov/node/1961.

U.S. Resilience Project. *Priorities for America's Preparedness: Best Practices from the Private Sector, Resilience Roundtable.* Washington, DC: October 31, 2011.

United Nations Development Group. *Socio-Economic Impact of Ebola Virus Disease in West African Countries: A call for national and regional containment, recovery and prevention*. New York, NY: United Nations Development Group—Western and Central Africa, February 2015.

United States Nuclear Regulatory Commission. "Backgrounder: Nuclear Insurance and Disaster Relief," June 2014.

van der Heijden, Kees. *Scenarios: The Art of Strategic Conversation*. New York, NY: John Wiley & Sons, 2011.

Vermont Emergency Management and Homeland Security. *Vermont State Emergency Operations Plan*. Vermont, US: Vermont Emergency Management, 2013.

Viollet-le-Duc, Eugène-Emmanuel. *Annals of a Fortress*. Translated by Benjamin Bucknall. Boston, MA: J. R. Osgood and Company, 1876.

———. *Dictionnaire raisonné de l'architecture française du XI. au XVI. siècle*. Paris, FR: Morel, 1869.

Viscusi, Kip. *Smoking: Making the Risky Decision.* Oxford, UK: Oxford University Press, 1992.

Warner, Edward P. "Present Conditions under the N.R.A." *American Marketing Journal* Vol. 1, No. 1, Jan., 1934, pp. 6–14.

Washington, DC Metropolitan Police Department. *After Action Report Washington Navy Yard September 16, 2013 Internal Review Of The Metropolitan Police Department Washington, D.C.,* Washington, DC: Washington, DC Metropolitan Police Department, July 2014.

Whitman, Walt. *Leaves of Grass Including a Facsimile Autobiography, Variorum Readings of the Poems and a Department of Gathered Leaves*. Edited by David McKay. Philadelphia, US: David McKay, 1891–1892.

Wilkinson, Angela and Roland Kupers. "Living in the Futures." *Harvard Business Review* 91, no. 5 (May 2013): 118–27.

Witherspoon, John. *The Works of John Witherspoon, D.D*. Edinbourgh, SCT: Ogle and Aikman, J. Pillans, J. Ritchie, J. Turnbull, 1805.

Wolfe, Thomas. *Look Homeward, Angel*. New York, NY: Simon and Schuster, 2006. First published in 1929 by Charles Scribner's Sons.

Wuthnow, Robert. *Be Very Afraid: The Cultural Response to Terror, Pandemics, Environmental Devastation, Nuclear Annihilation, and Other Threats*. New York, NY: Oxford University Press, 2010.

Yoran, Amit. "Escaping Security's Dark Ages." Speech. USA 2015 RSA Conference, April 21, 2015.

Zurara, Gomes Eannes de. *The Chronicle of the Discovery and Conquest of Guinea Vol. II*. Translated by Charles Raymond Beazley and Edgar Prestage. New York, NY: Burt Franklin, 1899.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California